Compliance Manual

November 2019

Table of Contents

1. INTRODUCTION

Purpose

Redhawk Wealth Advisors, Inc. (the **"Firm**") is an SEC Registered Investment Advisor ("**RIA**") and has adopted the following policies and procedures for compliance as an RIA under the Investment Advisers Act of 1940 ("**Advisers Act**"). Employees and Investment Advisor Representatives ("**IAR"** or collectively **"IARs**") of the Firm are expected to be familiar with and follow the Firm's policies.

Guidelines Only

The information and procedures provided within this manual represent guidelines to be followed by employees of the Firm, IARs, and employees of IARs ("**Supervised Person"** or collectively **"Supervised Persons**") and are not inclusive of all laws, rules and regulations that govern the activities of the Firm. Supervised Persons should conduct their activities in a manner that not only achieves technical compliance with this Compliance Manual, but also abides by its spirit and principles as a fiduciary.

The Chief Compliance Officer ("**CCO**") oversees the Firm's Compliance Committee, that is governed by a defined charter, and meets on a regular basis with the Compliance Committee to review and address compliance and/or supervisory issues of the Firm (collectively as "**Compliance**"). The CCO utilizes the services of other staff members of the Firm on an as needed basis for compliance purposes and to help the CCO in the on-going management of the Firm's compliance program ("**Designee**").

Questions

Any questions concerning the policies and procedures contained within this Compliance Manual or regarding any regulations or compliance matters should be directed to Compliance in writing and sent to compliance@redhawkwa.com.

Any reference needing review or approval from Compliance referenced in this document should be sent to compliance@redhawkwa.com.

Any reference needing review or approval from the operations team ("**Operations**") referenced in this document should be sent to operations@redhawkwa.com.

Any reference needing review or approval from the Firm's investment committee ("**IC**") referenced in this document should be sent to compliance@redhawkwa.com.

The CCO and Designee are identified below.

- Chief Compliance Officer: Rick Keast
- Chief Compliance Officer's Designee: Sarah Weigel

Acknowledgement

Supervised Persons are required to acknowledge that they have read and that they understand and agree to comply with the Firm's compliance policies and procedures.

Limitations on Use

The Firm is the sole owner of all rights to this manual and it must be either returned by the Supervised Person or electronically destroyed immediately upon termination of employment. The information contained herein is confidential and proprietary and should not be disclosed to any third-party or otherwise shared or disseminated in any way without the prior written approval of the Firm.

2. COMPLIANCE REVIEW

Objective of the Compliance Program

It is the policy of the Firm to remain compliant with all rules and regulations set forth by the Securities Exchange Commission ("**SEC**") and any other organization having governing authority over the Firm and its operations. As a result, the Firm has implemented the policies and procedures contained in this Compliance Manual and its Exhibits.

The Compliance Manual is designed to assist Supervised Persons in maintaining compliance with the securities laws under which the Firm operates, namely the Advisers Act as amended. The rules make it unlawful for any Supervised Person to provide advice to any client unless they have complied with the Advisers Act by:

1. Creating or adopting written compliance policies and procedures to address, at a minimum, the following areas:
   a. **Portfolio Management Processes:** Portfolio management processes, including allocation of investment opportunities among clients and consistency of portfolios with clients' investment objectives, disclosures by the Supervised Person, and applicable regulatory restrictions.
   b. **Trading Practices:** Trading practices that satisfies Best Execution obligation, uses client brokerage to obtain research and other services, and allocates aggregated trades among clients.
   c. **Proprietary Trading:** Proprietary trading of personal trading activities of Supervised Persons.
   d. **Disclosures:** The accuracy of disclosures made to clients and regulators, including account statements and advertisements.
   e. **Safeguarding Client Assets:** Safeguarding of client assets from conversion or inappropriate use.
   f. **Accurate Records:** The accurate creation of required records and their maintenance in a manner that secures them from unauthorized alteration or use and protects them from untimely destruction.
   g. **Marketing:** Marketing advisory services, including the use of solicitors.
   h. **Valuation Processes:** Processes to value client holdings and assess fees based on those valuations.
   i. **Privacy Safeguards:** Safeguards for the privacy protection of client records and information.
   j. **Business Continuity** Business continuity plans.
2. Creating a process to review written policies and procedures annually.
3. Designating a CCO.

Designation of Chief Compliance Officer

Rick Keast is designated as the Firm's CCO and is responsible for on-going compliance matters of the Firm. The CCO oversees the Firm's Compliance Committee, that is governed by a defined charter, and meets on a regular basis with the Compliance Committee to review

and address compliance and/or supervisory issues of the Firm. The CCO utilizes the services of other staff members of the Firm on an as needed basis for compliance purposes and to help the CCO in the on-going management of the Firm's compliance program. Such individuals report directly to the CCO. Ultimate responsibility for ensuring that its employees and Supervised Persons comply with the provisions of this manual and the federal and state securities laws resides with the CCO.

Designation of Responsibility

The CCO has full responsibility and authority to develop and enforce appropriate compliance policies and procedures and is responsible for all compliance functions. The CCO oversees the preparation and updating of the written policies and procedures contained in this Compliance Manual. The CCO ensures that a copy of these policies and procedures are maintained for a minimum of five (5) years from the date of the most recent change. The CCO or its Designee conducts annual audits and assessments of the business being conducted by the Firm and its Supervised Persons and updates its policies and procedures accordingly.

Duties of the CCO

Specific responsibilities and duties of the CCO include, but are not limited to, the following:

1. **Annual Review:** Reviewing the Firm's compliance policies and procedures at least annually (including any compliance matters that arose during the previous year) to determine the adequacy and effectiveness of the policies and procedures, and if necessary, updating the policies and procedures.
2. **Interim Reviews:** Conducting interim reviews in response to significant compliance events, changes in business arrangements, and regulatory developments.
3. **Compliance Training:** Conducting compliance training for new Supervised Persons.
4. **Testing and Monitoring Policies:** Drafting procedures to document the monitoring and testing of compliance through internal audits.
5. **Internal Assessment:** Implementing any policies needed to ensure that training and internal assessment procedures are updated to reflect changes in applicable laws, regulations, and administrative positions.
6. **Reporting of Breach:** Following up and resolving any reported breach of the Firm's policies and procedures.

Who is covered by the Firm's Compliance Program?

A Supervised Person is any associated person of the Firm that provides advice to clients or prospective clients. They are also any person with the capacity to affect a client's accounts at a custodian in any fashion. Under the Firm's current operational structure all associated persons of the Firm are considered Supervised Persons. A copy of this program outline and the policies derived under it is provided to each supervised Person. Each Supervised Person is required to acknowledge the receipt of this Compliance Manual and that they have read and fully understand the policies and procedures on an annual basis.

Areas of Coverage of the Compliance Program

On an annual basis, the CCO conducts a review of the business of the Firm, the types of clients it has, the types of investments made on behalf of its clients, and any other activities the Firm engages on a regular basis.

Annual Compliance Reviews. In addition, the CCO conducts an annual review of the Firm's policies and procedures to determine that they are adequate, current and effective in view of the Firm's businesses, practices, advisory services, and current regulatory requirements. The Firm's policy includes amending or updating the policies and procedures to reflect any changes in the Firm's activities, personnel, or regulatory developments, among other things, either as part of the Firm's annual review, or more frequently, as is appropriate, and to maintain relevant records of the annual reviews. The purpose of this review is to consider any changes in the Firm's activities, any compliance matters that have occurred in the past year, and any new regulatory requirements or developments, among other things. Appropriate revisions of a Firm's policies or procedures is made to help ensure that the policies and procedures are adequate and effective.

Procedures. Compliance adopts procedures to implement the Firm's policy and reviews to monitor and ensure the Firm's policy is observed, implemented properly and amended or updated, as appropriate and which include the following.

1. **Annual Review:** On an annual basis, Compliance undertakes a complete analysis of all Firm's written compliance policies and procedures.
2. **Subjects of Review:** The review includes a review of each policy to determine the following:
    a. Adequacy, effectiveness, and accuracy,
    b. Appropriateness for the Firm's current activities.
    c. Current regulatory requirements.
    d. Any prior policy issues, violations or sanctions.
    e. Any changes that are required or appropriate.
3. **Coordination of Review:** Compliance coordinates the review of each policy with the appropriate person, department manager, or officer to ensure that each of the Firm's policies and procedures is adequate and appropriate for the business activity covered, e.g., a review of the trading policies and procedures with the person responsible for the Firm's trading activities.
4. **Revision of Policy:** Compliance revises any of the Firm's policies and/or procedures as necessary or appropriate and obtains the approval of the person, department manager, or officer responsible for an activity as part of the review.
5. **Prior Violations or Issues:** Compliance's annual reviews includes an overview of any prior violations or issues under any of the current policies or procedures. This helps the Firm to avoid similar violations or issues in the future.
6. **Maintain Copies:** Compliance maintains hardcopy or electronic records of the policies and procedures as in effect at any time.

7. **Annual Compliance Review File:** Compliance maintains an Annual Compliance Review file for each year, which includes any revisions and materials supporting such changes and approvals, of any of the Firm's policies and/or procedures.
8. **Ad Hoc Reviews:** Compliance conducts more frequent reviews of the Firm's policies or procedures, or any specific policy or procedure, in the event of any change in personnel, business activities, regulatory requirements or developments or other circumstances requiring a revision or update.
9. **Risk Assessment:** Compliance conducts a risk assessment of the Firm's operation and update policies and procedures as warranted.
10. **Retention of Records:** Compliance maintains relevant records of such additional reviews and changes.

Regulatory Inspections

The Firm is examined by the Office of Compliance Inspections and Examinations ("**OCIE**") of the SEC. OCIE conducts exams out of Washington D.C. and each of the SEC's 11 regional offices. On the first day of the examination, the Firm shall be prepared for representatives from the SEC/OCIE to ask about or for:

1. A general overview of the Firm.
2. The type of Firm clients.
3. Services provided by the Firm.
4. Investment strategies employed and products offered by the Firm.
5. An overview of the marketing strategies and sales practices employed by the Firm.
6. A general description of the Firm's compliance program.
7. An explanation of how the Firm values clients' assets and how the Firm charges its advisory fees.

When the SEC, state securities commission or other regulatory agency contacts or meets a Supervised Person of the Firm, the following procedures are followed:

1. The Supervised Person of the Firm that was contacted by the SEC is required to immediately inform the CCO about the matter;
2. The CCO arranges for the Firm to make available all documents requested by the examiner, provided such examiner has the legal right to examine such documents;
3. The CCO reviews prior to the arrival of the inspection staff:
   a. If a surprise visit, the CCO asks the SEC official(s) for: (i) proper identification, (ii) their authority to conduct the examination, and (iii) the purpose of the visit;
   b. The CCO and any other Firm personnel chosen to assist the regulatory inspection team is required to be pleasant and cooperative;
   c. Information or copies of documents are provided to the official only if the release of such information or documents has been cleared by the CCO;
   d. The CCO ensures that only those documents specifically requested by the regulatory inspection team are released to the regulatory inspection team;
   e. A representative of the Firm always accompanies the regulatory inspection team when the team is in the Firm's office(s), except in a room or rooms designated by the CCO as places where the team can perform their inspection;

f. Without prior clearance from the CCO, no employee can have substantive conversations with any member of the regulatory inspection team;
g. Upon completion of the examination, the CCO asks a member of the SEC's inspection team the date when the examination will be completed. (Under the Dodd-Frank Act, the SEC has 180 days from the date of its document request to complete its examination of a registered investment advisor);
h. The recipient of any letter or other correspondence from the inspecting regulatory authority must promptly forward such correspondence to the CCO;
i. The CCO, in coordination with the legal counsel of the Firm or third-party compliance consultant, reviews the correspondence from the inspecting regulatory authority and responds, if so required, in the appropriate manner prior to any deadline imposed by the inspecting authority; and
j. If OCIE identifies deficiencies or weaknesses, the Firm takes steps to address and eliminate such deficiencies and weaknesses and memorialize the actions taken in a memorandum. If serious deficiencies are found, OCIE refers the problems to the SEC's Division of Enforcement, or to a self-regulatory organization, state regulatory agency, or other regulator for possible action.

3. REGISTRATION AND LICENSING

State Notice Filing Requirements

The Firm has been granted registration as an investment advisor ("**RIA**") with the SEC and is required to notice file in each individual state in which it is required to do so under the state statutes. Unless otherwise permitted by regulation, the Firm does not solicit or render investment advice for any client domiciled in a state where the Firm is not properly registered.

Registration of Investment Advisor Representatives

IARs refer to the individual agents associated with the Firm who render investment advice on behalf of the Firm. In general, states require either of the following of IARs: (1) Sitting for and passing the FINRA brokerage exam Series 7 and the Investment Advisor Examination Series 66, or the Investment Advisor Exam Series 65; or (2) a professional designation (CFA, CFP, or ChFC, PFS, etc.).

In addition, state registration requirements for IARs vary by state and can include: 1) Form U-4 for the IAR; 2) fingerprints, which are the responsibility of the IAR (unless current copy on file with the FINRA); 3) proof of examinations, and 4) filing fees to be submitted directly to the state (via the Firm's IARD Account). The Firm ensures that each of its IARs are adequately registered prior to allowing IAR business to be conducted by its IARs, on behalf of the Firm, in the relevant jurisdiction. State registration of IARs are made electronically via the IARD system.

No IAR can provide investment advice to any client until they have received notice from Compliance that they have been granted, as necessary, an investment advisor registration license/approval from the relevant state(s).

Registration Amendments: An IAR must immediately notify Compliance in writing if any information required by their Form U-4 becomes outdated. Depending upon what information has been updated, an amendment to the Form U4 can be required. If such an amendment is required, such filing is submitted with the appropriate jurisdiction via the IARD. Compliance contacts the IARs regarding updating their U4 on an annual basis.

Compliance ensures that, within thirty (30) calendar days of termination of any IAR from the Firm, a Form U-5 is filed with FINRA. Compliance also provides the terminated IAR with a copy of such Form U-5 within the same time frame. Any subsequent amendments to Form U-5 is also filed within thirty (30) days of Compliance learning of the need for such amendments. Initial filings and amendments of Form U5 are submitted electronically.

Supervisory Responsibility—State Registration

Compliance is responsible to be aware of the requirements of the states in which the Firm operates and to ensure that the Firm and its IARs are properly registered, licensed, and qualified to conduct business pursuant to all applicable laws of those states.

If the state requires fingerprinting, it is the IAR's responsibility to locate a proper organization that will take their fingerprints. The IAR is also responsible to ensure that the fingerprints are sent to the appropriate department of the state for review.

Third-Party - Compliance Consultant

The Firm retains a third-party consulting firm to assist with compliance related requirements and any issues that arise. The consulting firm also assists the Firm with submitting all appropriate filings on the Firm's behalf. Compliance is responsible for ensuring such filing requirements are met and obtains confirmation from the consulting firm that all required filings are completed.

Annual Renewal/Annual Updating Amendment

Compliance files (1) an annual renewal prior to year-end through the IARD, and (2) annual updating amendment via the IARD within ninety (90) days after its fiscal year-end.

Filing Fees

The state(s) to which the Firm is registered and has registered IARs charge fees, which are deducted from the IARD account established with FINRA. Compliance is responsible for maintaining required capital balances with FINRA to facilitate the payment of registration fees for the Firm and its IARD as well as annual renewal fees when they are due.

Hiring and Training of Investment Advisor Representatives

The Firm is responsible and has the duty to ascertain by investigation the good character, business reputation, qualifications, and experience of any person prior to making such a certification in the application of such person for association with the Firm. The Firm has a documented due diligence process when reviewing potential new IARs. The New Advisor Committee approves each due diligence phase before the Firm contemplates having the IAR join the Firm. Where an applicant for registration has previously been registered with a broker/dealer or other RIA, the Firm reviews the FINRA broker check website for a complete list of industry associations and any disciplinary history.

Ensure Proper Registration and License

To qualify as an IAR, it is necessary for the individual to:

1. Have passed all applicable state investment advisor representative examinations, unless the examination(s) has/have been waived; and
2. Unless exempt, be registered as an IAR of the Firm in all states where the individual conducts business activities. Passing an examination alone does not equate to licensure.

IARs of the Firm are prohibited from soliciting potential business from a prospective client or render any advice unless registered in the client's or prospective client's state of residence, unless exempt from registration. Questions regarding registration requirements should be directed to Compliance.

Representative Disqualification

The Firm does not permit a person who was not approved during the due diligence process to become associated with the Firm.

Records for all "Associated Persons"

The Firm maintains employment files for all associated persons of the Firm. "**Associated Persons**" are any partner, officer, director, or branch manager of such IAR (or any person occupying a similar status or performing similar functions), any person directly or indirectly controlling, controlled by, or under common control with such IAR, or any employee of such IAR, that has passed the investment advisor representative examinations. Any person associated with an IAR whose functions are solely clerical or ministerial shall not be included in the meaning of such term.

The Firm maintains the employment file by requiring all Associated Persons to complete a Form U4 and promptly update it, as applicable. Compliance maintains these files and makes sure that a complete and signed Form U4 is in each Associated Person's file.

Unregistered Supervised Persons

Compliance monitors the activities of unregistered Supervised Persons. Unregistered Supervised Persons are prohibited from conducting any investment advisory business without proper licensure. Unregistered Supervised Persons are authorized to only participate in the following:

1. Clerical or administrative matters concerning client accounts.
2. General discussion of the services offered.
3. Refer clients to an IAR of the Firm for more specific information concerning account(s).
4. Provide prospective clients with approved marketing brochures or materials.
5. Amend brochures or brochure supplements along with a (i) statement describing the material facts relating to the change in the disciplinary information, or (ii) a statement describing the material facts relating to the change in disciplinary information.
6. File Forms U-4 and U-5 with FINRA.
7. File the annual update annual amendment
8. File (i) an annual renewal prior to year-end through the IARD, and (ii) annual updating amendment via the IARD within ninety (90) days after its fiscal year-end.

Review and Amendments to Form ADV

The CCO reviews the Firm's Form ADV on an ongoing basis to ensure that all information is current and accurate. The Firm's Form ADV is amended within 30 days when changes have been made to the Firm's policies and procedures or upon discovery of an inaccuracy in the following Items: 1, 2, 3, 4, 5, 8, 11, Schedule A and Schedule B of Part 1 of Form ADV.

Disciplinary Disclosure

All material facts relating to legal or disciplinary events are disclosed in writing to existing clients promptly after the legal or disciplinary event occurs.

Required Disclosures

The Firm discloses any facts or circumstances which reasonably impact the Firm's or its affiliates' ability to meet their contractual commitments to clients. Examples of information that must be disclosed include:

1. The likelihood of bankruptcy or insolvency.
2. An event that would occupy the Firm's time so that its ability to manage client assets would be impaired.
3. An event that is material to an evaluation of the Firm's or its affiliates' integrity or their ability to meet contractual commitments to clients.

Solicitor/Referral Relationships

The Firm does not have solicitor/referral relationships and it does not compensate third parties for client referrals.

Responsibility

The CCO is responsible for the implementation and monitoring of the Firm's solicitation policies, practices, client disclosures, and recordkeeping.

Privacy Notice Disclosures

At the inception of the client relationship, IARs are required to provide a copy of the Firm's privacy notice, as set forth in the Privacy Policy section of this manual. The Firm does not share non-public personal information with non-affiliated third parties. If the Firm has not changed its Privacy Policy from the most recent Privacy Policy that were disclosed to clients, the Firm won't provide the same Privacy Policy to clients on an annual basis. The Firm only sends an annual Privacy Policy, notifying clients of the change, when the Privacy Policy has been changed during the year.

Proxy Voting Disclosures

At the inception of the client relationship, IAR's are required to provide information disclosing that the Firm does not vote proxies. This disclosure is in Part 2A of the Form ADV and the advisory agreement.

FORM 13-H

If the Firm meets the definition of a large trader, it must register with the SEC by filing and periodically updating Form 13H through the SEC's EDGAR system. The term "**Large Trader**" is defined as any person that: i) directly or indirectly, including through other persons controlled by such person, exercises investment discretion over one or more accounts and effects transactions for the purchase or sale of any National Market System ("**NMS**") security for or on behalf of such accounts, by or through one or more registered broker-dealers, in an aggregate amount equal to or greater than the identifying activity level; or ii) voluntarily registers as a large trader. NMS securities are generally U.S. exchange-listed securities, including equities and options. Currently, identifying activity level means aggregate transactions in NMS securities that are equal to or greater than: 1) during a calendar day,

either two million shares or shares with a fair market value of $20 million; or 2) during a calendar month, either twenty million shares or shares with a fair market value of $200 million. With respect to options, their volume and value for identifying activity level purposes are based on the underlying securities referenced (e.g., 500 XYZ call options would count as aggregate transactions of 50,000 shares in XYZ).

If the Firm meets the Large Trader definition, it must file an initial Form 13H within 10 days after effecting aggregate transactions equal to or greater than the identifying activity level. Additionally, all Large Traders must submit an annual filing of Form 13H within 45 days after the end of each full calendar year. If any of the information contained in a Form 13H filing becomes inaccurate for any reason, a Large Trader must file an amendment no later than the end of the calendar quarter in which the information became stale. Additionally, if the Firm meets the Large Trader definition, it must disclose to the registered broker-dealers effecting transactions on its behalf its large trader identification number ("**LTID**") and each account to which it applies.

FORM 13-D, 13F, 13G

Compliance provides reports required by Section 13(d), 13(f), and 13(g) of the Securities Exchange Act of 1934 prepared and filed on a current basis. Form 13D reports are for any person who acquires directly or indirectly beneficial ownership of more than 5% of any equity security with either the intent or effect of causing a change in control. Compliance files Form 13G if the Firm acquires more than 5% of any equity security without the purpose of changing or influencing control of the issuer. Compliance files Form 13(f) because the Firm manages more than $100 million in securities of companies admitted to trading on a national securities exchange or quoted on the automated quotation system of a registered securities association, as provided in Section 13(f) of Securities Exchange Act of 1934.

4. BOOKS AND RECORDS

Responsibility

The Firm creates and preserves records relating to its activities, to transactions for client accounts, to personal securities transactions of its personnel, and to a variety of other matters. In addition to these requirements, the Firm's books and records adhere to the provisions of the Privacy Policy and Written Information Security Policy sections of this manual below.

Compliance, on an annual basis, reviews the Firm's records and destroys any that have become obsolete. A record becomes obsolete when they are older than the required retention requirements (as further set forth below). Supervised Persons are prohibited from falsifying, tampering, destroying these records. Doing any of the aforementioned, could subject the Supervised Person to criminal penalties, regulatory sanctions, and/or termination of employment.

Any questions about these matters should be directed to Compliance.

Retention Requirements

The Firm keeps and maintains certain books and records for the periods of time described in Retention of Books and Records in Appendix A, attached hereto and incorporated herein by reference. This section applies in conjunction with the Performance Advertising Records and Electronic Communications Policy sections below.

Specific Record Keeping Requirements

The Firm maintains its books and records as described below:

1. **Cash Journal:** A journal or journals, including cash receipts and disbursements records, and any other records of original entry forming the basis of entries in any ledger.
2. **Ledgers:** General and auxiliary ledgers reflecting assets, liabilities, reserve, capital, income, and expense accounts.
3. **Buy/Sell Orders:** A record of each order given by the Firm for the purchase or sale of a security. Trade records are retained electronically and show the terms and conditions of the order (buy or sell) and shall:
    a. Show any instruction, modification or cancellation.
    b. Identify the person connected with the Firm who recommended the transaction to the client.
    c. Identify the person who placed the order.
    d. Show the account for which the transaction was entered.
    e. Show the date of entry.
    f. Identify the bank, broker or dealer by or through whom such order was executed.
    g. Identify orders entered into pursuant to the exercise of the Firm's discretionary authority.
4. **Banking Records:** Check books, bank statements, canceled checks, balance sheets, and cash reconciliations.

5. **Bills and Statements:** All bills, invoices, or statements, whether paid or unpaid, relating to the business of the Firm.
6. **Financial Statements:** Trial balances, financial statements, and internal audit working papers.
7. **Communications from Clients:** Written communications received from clients, either in hard copy or electronic format.
8. **Communications to Clients:** Written communications sent to clients, either in hard copy or electronic format.
9. **Clients and Accounts:** A list of clients and accounts over which the Firm has discretion.
10. **Discretionary Authorizations:** Executed discretionary power authorization forms.
11. **Ads:** Advertisements, including copies of the Firm's website.
12. **Holdings/Posting Page:** A record of every transaction in a security in which the Firm holds a direct or indirect ownership interest.
13. **Disclosure Documents:** Form ADV Part 2A, 2B, and every amendment.
14. **Annual Disclosures:** Copy of Annual Offer of Disclosure Document. Include a list of clients/investors who were sent the offer of the Disclosure Document, and a list of those who requested copies of the Disclosure Document.
15. **Contracts:** Written agreements entered by the Firm and maintained for a period of five (5) years or more after termination of relationship).
16. **Client Complaints:** Client complaint file that is maintained even if empty.
17. **Policies and Procedures:** Copies of the Firm's policies and procedures and any amendments thereto.
18. **Performance Advertising Supporting Documents:** All accounts, books, records, and documents necessary to form the basis for calculation of performance or rate of return of managed accounts or securities recommendations in any Firm communications distributed to ten (10) or more persons; for example, if a Firm distributes performance numbers from the year 1996-2012, the Firm must maintain documents, i.e. brokerage statements from each client account included in the composite necessary to show the calculation for each return back to 1996. Thus, the five-year retention rule does not apply to performance advertising.
19. **Code of Ethics Policy:** Copies of the Firm's Code of Ethics currently in effect or that was in effect any time within the last five (5) years, including (a) records of any violations of the Code of Ethics and any actions taken as a result of the violations; (b) records of all written acknowledgements of receipt of the Code of Ethics for each person who is currently or has been within the last five (5) years a Supervised Person of the Firm; c) annual records of all written acknowledgements of compliance with the Code of Ethics for each person who is currently or has been within the last five (5) years a Supervised Person of the Firm; and (d) a list of all Supervised Persons together with records of all Supervised Persons during the last five (5) years.
20. **Personal Securities Transactions:** Records of all Personal Securities Transactions for Supervised Persons as defined in the Firm's Code of Ethics.

Corporate Records

The Firm maintains accurate and current organizational documents. The CCO is responsible

for implementing and monitoring the Firm's organizational documents policy, practices, and recordkeeping. The CCO, on an annual basis, reviews the organizational documents to ensure the Firm's policy is implemented properly, and updated, as appropriate.

The CCO maintains the organizational documents in a secure fireproof filing cabinet, located in their office. All organizational documents reflect current directors, officers, members or partners, as appropriate. The CCO maintains the organizational documents for a period of three (3) years or more after termination of the Firm's existence. The organizational documents are maintained with reasonable access, the address of such location shall be communicated to the proper regulatory authority upon the required filing of Form ADV-W (the form used to withdraw registration as an RIA with the SEC) and any change in the location of such records are promptly communicated to the proper regulatory authority.

Organizational documents include the following:

1. Organization Agreements.
2. Articles of Incorporation.
3. Charters.
4. Minute books.
5. Stock certificate books/ledgers.
6. Organization resolutions.
7. Any changes or amendment of the organization documents.

E-Mail Retention

Compliance maintains a record of all e-mails that pertain to advice being offered, recommendations being made, transactions executed, and orders received. Compliance arranges and indexes such communication like any other electronically stored record and in accordance with its Written Information Security Policy (see below). This is done in such a manner that permits easy location, access, and retrieval. The Firm outsources its email archiving to Smarsh.

If requested by any regulatory authority, Compliance will provide a legible, true, and complete copy of e-mails in the medium and format in which it is stored.

All such correspondence is kept for a period of at least five (5) years. Compliance reviews e-mail correspondence on a weekly basis and is required to provide such reviews to the CCO, as required. Compliance reviews this process at least annually pursuant to SEC rule requirements.

The Use of Electronic Media to Maintain and Preserve Records

1. **Permitted Use**. The Firm maintains all records electronically and the records are backed up daily.
2. **Requirements.** The Firm adheres to the following for storing records electronically:
   a. Maintains a duplicate backup copy of electronically stored books and records at an off-site location;

b. Organizes the records to permit immediate location and retrieval;
c. Is ready to promptly provide records to an examiner;
d. Verifies the quality and accuracy of the storage media recording process;
e. Maintains the capacity to readily download records; and
f. Provides a means to access, view, and print records.

3. **Access and Regulatory Requests.** The Firm is prepared, upon request by any regulatory authority, to promptly provide (i) legible, true, and complete copies of these records in the medium and format in which they are stored, as well as printouts of such records; and (ii) a means to access, view, and print the records.
4. **Security.** All Supervised Persons with access to client records are prohibited from leaving their computers on when unattended. Such Supervised Persons must either shut down their computers or put their computer in sleep mode before leaving their computer. Compliance takes the necessary steps to assure that whenever a Supervised Person leaves the Firm any password or code used to gain access to that computer system, any third-party application, or e-mail is extinguished or changed.

Branch Office and IAR Private Office Records

The Firm's branch offices and IAR private offices are prohibited from keeping the following:

1. Books and records required to be maintained by the Firm.
2. Any record or document that is necessary to form the basis for or demonstrate the calculation of performance or rate of return of any or all managed accounts of a Supervised Person while at a prior firm.

Supervised Persons are required to:

1. Provide Operations an electronic copy of the client records no later than one (1) week from the creation or receipt of the record.
2. Provide the email policies and procedures and encryption capabilities if using a Firm approved DBA email.
3. Send business-related email communication using their redhawkwa.com email or Firm approved DBA email address through the Firm's email system, which is captured and stored by the firm.
4. Include the word "Confidential" in the subject line when sending a business email with confidential information. The Firm's email system encrypts any email that has the word "Confidential" in the subject line and is being sent by a redhawkwa.com email or Firm approved DBA email address.
5. Make available, upon request, any material notes in relation to a client.
6. Use the Firm's most current approved version of Form ADV, Investment Policy Statement ("**IPS**") or a similar Firm approved document, advisory agreement(s), rollover checklist (if applicable), and financial consulting and planning agreement (if applicable) when sending these documents to clients. Supervised Persons are prohibited from creating local copies of these documents, as they can change at any time. Supervised Persons are required to use the current version from the Firm's web site, or third-party web site (if applicable) with each use. Additionally, Supervised Persons are prohibited from creating customized or revising versions of these documents for their use, unless an alternative version is

authorized in writing by Compliance.

7. Document all deliveries of Form ADV to clients or prospective clients and is required to record when and to whom Form ADV was delivered to clients or prospective clients.
8. Submit a record of any checks received onto the office check log upon receipt. Receipt of checks made payable to clients or client checks payable to the client's custodian are subject to the Firm's custody policies and procedures (See Custody section).
9. Distribute only Firm approved marketing materials (See Advertising section).

The branch offices and IAR private offices are aware that regulators have the authority to inspect the books and records of their offices at any time. The branch offices and IAR private offices are required to notify the CCO immediately if anyone at an office is contacted by a regulator. The branch offices and IAR private offices keep duplicate copies of records and return all original documents to the client for servicing purposes.

Branch Office and IAR Private Office Inspections

1. Compliance conducts off-site examinations of these offices every year. The CCO or Designee conducts on-site inspections of these offices every three (3) years with exception of new IAR' which are inspected within their first calendar year. Office inspections include internal review activity, testing, and verification of policies and procedures, in the areas of:
   a. Safeguarding client funds, securities, and records.
   b. Maintaining required books and records.
   c. Quarterly reporting records.
   d. Annual reporting records.
   e. Electronic communications.
   f. Data protection.
   g. Advertising and marketing.
   h. Internal records, including client complaints.
   i. Personal and client trading activity.
   j. Validating client account information and disclosure deliveries.
2. Each office inspection is documented in a written report and kept on file for a minimum of five (5) years. The written report addresses any findings or violations relating to the above policy areas and any other material violations.
3. The Firm adheres to the follow following procedures when documenting the office inspection reports:
   a. A copy of the branch inspection report is given to the manager of the branch office or IAR.
   b. Compliance maintains these reports and the manager of the branch office or IAR is required to take corrective measures or direct corrective measures to be taken where required based on the reports.
   c. The dates of the audit/review and the names of the individuals conducting the review is included with each report.
   d. The manager of the branch office or IAR is required to make all corrective and remedial actions.
   e. The manager of the branch office or IAR is required to provide written confirmation to

Compliance that all corrective and remedial actions have been completed and document the corrective action.

f. The CCO determines whether a branch office or IAR private office subsequent review date be moved up, whether to undertake a surprise inspection or any other proactive compliance measures deemed appropriate based on the report.
g. Compliance maintains notes relating to the above and indications of all steps taken to confirm that required measures were taken.

5. CLIENT REPORTING

Introduction

The valuation of portfolio holdings impacts client portfolio reporting, fee calculation, and performance calculation processes. Supervised Persons are required to accurately report client account values and performance.

Policies

1. The Firm provides clients portfolio reports that reflect accurately the value of accounts managed. If the Firm is unable to obtain a readily available market value for a security, the Firm discloses to the client the valuation method used for reporting and fee billing. If the Firm is unable to obtain a current value for a security, the Firm discloses to the client the frequency of the valuation of the security.
2. The Firm purchases securities with readily available market prices for clients, and the Firm uses the securities prices provided by the client's custodian to value client accounts.
3. In certain circumstances, such as annuities held in client accounts, pricing is obtained from the annuity provider.

Procedures and Responsible Party

1. The Firm and Orion (a designated third-party) is used to provide quarterly performance statements to clients. The CCO conducts periodic reviews of services performed for accuracy and consistency.
2. The following tasks are performed to produce the quarterly performance statements for the client:
   a. Orion downloads all client transactions, holdings, and account values from custodians on a nightly basis.
   b. The Firm reconciles accounts daily and resolves any discrepancies.
   c. Orion calculates the composite performance returns on a monthly basis, based on the Firm's criteria.
   d. Orion calculates the advisory fees on a monthly basis, based on the Firm's criteria.
   e. The Firm generates performance statements for clients on a quarterly basis.
   f. The Firm reviews all quarterly performance statements prior to distribution to the client and promptly corrects any discrepancies.

Recordkeeping

The Firm maintains an electronic copy of the quarterly performance statements provided to clients.

6. ADVISORY FEE BILLING PRACTICES

Policies

1. The Firm charges advisory fees based on the fees stated in the advisory agreement.
2. The Firm discloses the standard fee schedule to clients and prospective clients in its ADV Part 2A and records client's specific fees, including any agreed-upon fee concessions, in the advisory agreement.
3. The Firm calculates the advisory fees in arrears as a percentage of assets under management on a monthly basis, based upon the average daily balance during the previous month.
4. The Firm reserves the right to negotiate advisory fees with clients and can charge lower fees than the maximum fee described in the Firm's brochure.
5. The Firm does not share any advisory fees with any person as stated in its ADV Part 2A.
6. The Firm has not entered into an arrangement for a share of the Firm's advisory fees.
7. The Firm notifies clients of the advisory fees on the quarterly performance statements or by invoice if the client is paying the Firm directly.
7. The Firm debits client's accounts directly for the advisory fees only for those clients that have signed the advisory agreement.
8. The Firm debits advisory fees from the client accounts once the daily reconciliation is completed without any discrepancies and security prices have been reviewed.
9. The Firm does not debit advisory fees for accounts that went to zero during the month.

Procedures and Responsible Party

1. Orion calculates the advisory fees, based on the Firm's criteria, and completes the reconciliation and valuation process as described above.
2. Operations reviews a sampling of client accounts to ensure the advisory fees are calculated accurately prior to debiting the advisory fees.
3. Third-party investment managers that custody client accounts calculate the advisory fees and debits client accounts. Operations reviews a sampling of advisory fees for accuracy.
4. The Firm adheres to the following procedures and:
    a. Confirms that Orion has reconciled all client accounts;
    b. Reviews a sampling of fee calculations performed by Orion to confirm accuracy prior to an invoice being sent to a client or the client's account being debited;
    c. Maintains all necessary records documenting the fees billed to clients.
    d. Ensures that billing reviews are done for all new accounts, and all accounts with unique or unusual circumstances, and on a sampling basis for all other accounts;
    e. Provides approval to Orion of the fee calculation before Orion send the fee files to the Qualified Custodians to debit the client accounts;
    f. Promptly resolves any discrepancies;
    g. Reviews advisory fees received against advisory fees billed; and
    h. Maintains necessary records documenting the fees billed to client, and records of all reviews performed.

5. Supervised Persons are responsible for the accurate billing of clients that have signed a financial planning agreement. Supervised Persons are required to adhere to the following:
   a. Confirm the financial planning fee amount is consistent with the terms of the agreement.
   b. Provide the name and email address of the client to Operations so they can directly invoice the client and the client can pay for the service with their credit card using the Firm's third-party secure payment application. The Firm and the Supervised Person do not have access to the client's credit card information.
   c. Keep complete and accurate records of invoices and payments.
   d. Operations reconciles invoices and payments and communicates any discrepancies to the Supervised Person.

Recordkeeping

Operations maintains records documenting all fees billed to client, all fees received, invoices sent to clients, refunds calculated, and any other applicable documentation.

Double Dipping Policy Restriction

If an IAR has a current, or previous relationship with a broker-dealer, the Firm prevents "**Double Dipping**." Double Dipping occurs when a financial professional, such as a registered representative, places commissioned products into a fee-based account and then makes money from both the commission and the fee.

IARs are prohibited from earning a commission and advisory fee on the same assets within a comparable time period. In order to prevent this, Operations:

1. Reviews the holdings of client accounts on quarterly basis and determines which clients hold a commission based mutual fund.
2. Notifies the custodian of the account and instructs the custodian to convert the commission based mutual fund to a non-commission based mutual fund (commonly known as institutional or "I" share class). This type of mutual fund share class conversion can typically be done by the custodian without affecting the cost basis of the account or charging any type of fee to the client.
3. Reviews the client's account to ensure that the transfer has taken place.

7. CUSTODY

Introduction

There are rules that set forth extensive requirements regarding possession or custody of client funds or securities. In addition to the provisions of these rules, many states impose special restrictions or requirements regarding custody of client assets. The Firm is responsible for monitoring these requirements.

Responsibility

The Firm does not maintain possession or custody of client funds or securities.

Definition of Qualified Custodians

"**Qualified Custodians**" include the types of financial institutions that clients and Supervised Persons customarily turn to for custodian services. These also include banks and savings institutions, registered broker-dealers, and registered futures commission merchants among others. The Qualified Custodian is responsible for the safekeeping of the client's funds and securities.

Deduction of Advisory Fees from Client Accounts

Advisory fees are debited directly from the client accounts. Payment of the advisory fees are made by the Qualified Custodian. In all such cases, the client provides written authorization (such as an advisory agreement or letter of instruction) permitting the fees to be paid directly from their account. The Firm does not have access to client's funds for payment of fees without the client's consent in writing. The Qualified Custodian delivers a monthly or quarterly account statement directly to the client, and never through the Firm.

Inadvertent Receipt of Funds or Securities

The Firm prohibits and does not accept receiving client's funds for any reason. If the Firm inadvertently receives client funds or securities, Operations immediately takes the following steps to correct this action and not assume custody:

1. Operations makes a record of the receipt of client funds and/or securities. A notation of the receipt of the funds/securities received including the name of person who received the funds or securities, client name, date received, amount of the funds or name of the security, number of shares or face value of such security, coupon and maturity date (if applicable) as well as the date the funds/securities were returned to the sender and how they were returned.
2. Operations photocopies the check or securities received and places the photocopy in the client's file.
3. Operations either forwards the client funds or securities to the appropriate custodian or returns the funds/securities to the sender with a letter of instruction on how and where the sender should forward funds/securities in the future. Operations sends such funds or securities by U.S. Mail, registered, return receipt requested or by courier service within three business days of receipt of the funds/securities.

4. Operations keeps a copy of the cover letter and the return receipt/courier notice in the client's file.

Receipt of Third-Party Funds

If the Firm receives a check from a client payable to a third-party, Operations makes a photocopy of the check, issues a receipt to the client, and then forwards the check directly to the third-party. A copy of the check and the receipt are kept in the client's file.

Notice of Qualified Custodian

When Operations opens an account with a qualified custodian on behalf of the client, the Qualified Custodian notifies the client in writing of the Qualified Custodian's name, address and manner in which the client funds or securities are maintained promptly when the account is opened and following any changes to this information.

Account Statements

The Firm arranges for the client to receive monthly or quarterly account statements from the Qualified Custodian ("**Account Statement**") containing at least the information required by the applicable SEC and State rules directly to the client. The Firm uses Orion to create the client's quarterly performance statement that includes account values, holdings, and account performance ("**Supplemental Reports**"). The Supplemental Report are stored on the Orion system and are accessed by the Supervised Person and client. The Supervised Person is responsible to forward the Supplemental Report electronically to the client.

Responsibility

The CCO is responsible for having a reasonable belief that the Qualified Custodian delivers Account Statements directly to the clients either monthly or quarterly. Operations is responsible for ensuring that the Firm transmits accurate Supplemental Reports where agreed upon with clients quarterly.

Procedures

Where the Firm has agreed to prepare Supplemental Reports, the Firm prepares each Supplemental Report as agreed to with the client.

Supplemental Report Accuracy Review

Operations is responsible for reviewing Supplemental Reports for accuracy.

Address Changes

When a client requests a change of address, the Qualified Custodian sends out a letter or email verifying the change of address to the client at both the old and new address. Supervised Persons are responsible for ensuring that Operations and the Qualified Custodian have the current address on file for its clients.

Books and Records

Operations stores each client's Supplemental Report on the Orion system.

Use of an Independent Representative

Supervised Persons are required to have their client submit a request in writing if they do not wish to receive Account Statements. Supervised Persons are required to have the client to designate an independent representative in writing to receive the statements. Supervised Persons are required to forward documentation of such request to Operations. All such requests are stored in the client's file.

Supervised Person as Trustee

The Firm prohibits any Supervised Person to serve as a trustee except in situations where there is a family relationship with the grantor or beneficiary.

Standing Letters of Authorization

The Firm prohibits clients from using third-party Standing Letters of Authorization ("**SLOA**" or collectively "**SLOAs**"). The Firm allows SLOAs for like-titled accounts.

8. MONITORING OF INDEPENDENT INVESTMENT MANAGERS

Policy

The Firm's Investment Committee ("**IC**") is governed by a charter and monitors other registered investment advisors who, at the recommendation or direction of the Firm: (i) act as independent third-party investment managers for the Firm's clients or (ii) sponsor investment management programs that the Firm's clients can utilize ("**Independent Manager**" or collectively referred to as "**Independent Managers**") for compliance with the Rules.

Responsibility

The IC is responsible for conducting the due diligence and approving the initial and continued use of Independent Managers by the Firm. Once approved by the IC, the IC is responsible for monitoring the services of the Independent Manager.

Procedures

The IC conducts due diligence on an Independent Manager before approving an Independent Manager for use by clients of the Firm. The IC maintains a due diligence file on the Independent Manager. The due diligence file contains the Independent Manager's disclosure documents, performance returns, and any other information that the IC deems necessary.

On an annual basis, the IC monitors the services of the Independent Manager to ensure they are a suitable choice for the Firm's clients based on criteria the IC deems relevant. The criteria include, at a minimum, a review of the Independent Manager's disclosure documents, performance returns, personnel changes, and any other material information reasonably available which addresses the Independent Manager's ability to operate its business or provide quality services to the Firm's clients.

Books and Records

IC maintains documents evidencing the due diligence performed for the selection and monitoring of Independent Managers.

9. ANTI-MONEY LAUNDERING ("AML")

General Policy

The Firm does not engage in or facilitate any transaction with any person(s) or entity(ies) listed on the web site maintained by the Office of Foreign Assets Control ("**OFAC**") (www.treas.gov/ofac) relating thereto ("**Prohibited Person**"). However, since the Firm does not handle or maintain custody of clients' funds or securities, money laundering is only a minor concern. The Firm solely relies on the account review done through the Qualified Custodian to provide compliance with AML provisions. If the Firm learns that any Prohibited Person is, or is attempting to become, involved in any transaction with respect to the services which the Firm provides, Operations immediately reports such transaction to the Qualified Custodian and OFAC.

10. PROXY VOTING/CLASS ACTION LAWSUITS

Proxy Voting

The Firm does not vote proxies on behalf of clients and the Firm does not answer any proxy questions from clients. The Firm prohibits a Supervised Person to vote proxies on behalf of clients. Clients receive proxy material directly from the custodian holding their account.

Class Action Lawsuits

The Firm does not take any action or render any advice as to materials relating to any class action lawsuit involving a security held in a client's account.

11. ADVERTISING

Regulation

The Firm's advertising practices are regulated by strict rules and regulations, which prohibits the Firm from engaging in fraudulent, deceptive, or manipulative activities. These rules also prohibit the making of any material omission or any statement that is otherwise false or misleading. In reviewing advertisements by Supervised Persons, the SEC and state examiners look at the effect that an advertisement might have on careful and analytical persons and review the advertisements possible impact on those unskilled and unsophisticated in investment matters.

Definition of Advertising

Advertising is defined to include: "any written communication addressed to more than one person, or any notice or announcement in any publication or by radio, television, or electronic media which offers securities analysis or reports or offers any advisory services regarding securities." This broad definition includes standardized forms, form letters, the Firm's brochures, or any other materials designed to maintain existing clients or to solicit new clients.

The following are deemed to be an advertisement or marketing piece (NOTE: the following is not an all-inclusive list of what is considered advertising):

1. Marketing brochure.
2. Advertisement in a magazine or other publication.
3. Television, radio or broadcast advertisement.
4. Internet website.
5. E-mail sent to multiple recipients.
6. Audio/video of presentation designed to market.
7. Press releases.
8. Third-party publication reprints.
9. Performance presentations to more than one prospective client.
10. Telemarketing scripts.
11. Analysis, report, or publication concerning securities.
12. Verbal conversations via in person, telephone, or otherwise.
13. Written communication responding to an unsolicited request.
14. Account statements.
15. Academic articles.

Review and Approval

Supervised Persons are required to have each marketing piece or advertisement reviewed by Compliance and approved in advance of public dissemination.

With respect to each proposed advertisement or other marketing piece:

1. The Supervised Person submits the proposed advertisement to Compliance for review and the review request must include the following:
   a. The actual advertisement, if applicable.
   b. Text of the proposed advertisement.
   c. Target audience.
   d. Deadline.
   e. Statement whether the advertisement contains performance data.
2. Compliance determines whether the proposed advertisement in fact meets the definition of advertisement. Oral communications are not advertisements; however, fraudulent or misleading oral statements are prohibited.
3. If the advertisement contains performance returns, Compliance reviews documentation including worksheets supporting the calculation of the performance returns.
4. Compliance adheres to the factors described below, to determine whether the proposed advertisement is misleading, incomplete, inaccurate, or missing necessary information and that it complies with all applicable regulations and SEC interpretative positions of those regulations.
5. Compliance ensures that the advertisement contains the correct disclosures and disclaimers.
6. Compliance indicates their approval or disapproval on the proposed advertisement.
7. If disapproved, Compliance returns the proposed advertisement to the Supervised Person with comments and suggested edits.
8. If approved, Compliance notifies the Supervised Person that the proposed advertisement has been approved and Compliance stores the advertisement in the Supervised Person's file.
9. Supervised Persons are prohibited from modifying approved advertisements without the written approval of Compliance.
10. Advertisements that have been in use for at least one year are required to be sent through the process set forth above.

Review and Approval

Compliance reviews all Firm advertising and marketing documents prior to those documents being utilized by the Firm in any capacity. Compliance reviews all Supervised Persons advertising and marketing documents prior to those documents being utilized in any capacity. Documentation of all such marketing pieces and the approvals are maintained by Compliance.

Prohibited References

1. Use of the term "**Investment Counsel**."
   Supervised Persons are prohibited from using the term Investment Counsel in association with their business or services.
2. Use of the term "**RIA**."
   Supervised Persons are prohibited from using the term RIA after their name.
3. Use of the term "**Fiduciary**."
   Supervised Persons are prohibited from using the term Fiduciary after their name.

4. **Other Prohibitions.**
   The Firm does not represent that it has been sponsored, recommended or approved, or that its abilities or qualifications have been passed upon by any federal or state governmental agency.

Testimonials

The Firm or Supervised Persons are prohibited from using testimonials in any marketing materials. A testimonial includes a statement by a present or former client that endorses the Firm or Supervised Person and/or refers to the client's favorable investment experience. Supervised Persons are required to have Compliance approve the use of any third-party testimonials or ratings.

Third-Party Reports

The Firm can use bona fide and unbiased third-party reports, even if the Firm has paid the third-party to verify its performance.

Use of Advisory Client List

Supervised Persons are prohibited from using client information, in any manner, in an advertisement.

Use of Hedge Clauses

1. **Permitted Use.** Advertisements, correspondence, and other literature generated by the Firm can contain hedge clauses or legends that pertain to the reliability and accuracy of the information furnished.
2. **Disclosure.** The following disclosure must be provided when using hedge clauses: "The information contained herein has been obtained from sources believed to be reliable, but the accuracy of the information cannot be guaranteed."
3. **Restrictions.** Under no circumstances shall any legend, condition, stipulation or provision be written to create, in the mind of the investor, a belief that the person has given up some or all their legally entitled rights or protections.

Performance Presentations in the Firm Advertisements.

1. **General Legal Framework**
   The Advisers Act contains the basic antifraud provisions that govern Supervised Persons and certain specific prohibitions and restrictions on certain advertising practices (e.g., the use of testimonials; publication of guidelines concerning presentation of past specific recommendations; use of graphs, charts and formulas, etc.).
2. **Fees and Expenses**
   The Firm uses Orion to calculate the composite returns using a time-weighted rate of return ("**TWR**") adjusted for external cash flows. Composite returns are calculated by asset-weighting the individual portfolio returns using beginning-of-period values and external cash flows. All composite returns are calculated after the deduction of actual trading expenses incurred during the period. The Firm currently has only one portfolio in each composite and includes all discretionary fee-paying accounts that are managed

according to a strategy. In Orion, composite returns are calculated monthly, using trade date accounting, and are based on the portfolio fair value on the last day of the calendar month. More information as to how the Firm calculates composite returns can be found in the Firm's Composite Returns Policies and Procedures.

3. **Required Disclosures to Be Used with Gross Performance.**
   Any use of gross performance information must include the following disclosures:
   a. Results do not include advisory fees.
   b. A client's return is reduced by fees and other expenses.
   c. Fees are described in Part 2A of the Firm's Form ADV.
   d. An example showing the compounding effect of fees over a period of years. This can take the form of a table, chart, graph, or narrative.
4. **Required Disclosures for Performance Advertising**
   Any performance advertising must include adequate information on the following:
   a. Effect of material market or economic conditions on results.
   b. Effect of reinvestment of dividends and gains.
   c. Probability of loss if potential for profit is suggested.
   d. A description of any index used and of all relevant differences and similarities in cases of index comparisons.
   e. Material investment objectives and strategies.
   f. If using actual performance, a prominent disclosure that results only represent certain clients, the basis for selecting the limited group, and the effect of such selection.
5. **Recordkeeping Requirements**
   a. **Copies of Advertisements.** A copy of each advertisement sent to ten (10) or more people is kept for five (5) years in an easily accessible place.
   b. **Back-up for Performance Information**. A copy of the comprehensive account statements for all accounts included in advertisements and the worksheets used for all related performance calculations is kept for the same time period and in the same manner as the advertisements themselves.

Third-Party Rankings or Awards.

The Firm allows the use of third-party rankings or awards by its Supervised Persons. Supervised Persons must have Compliance approve the third-party rankings or awards and Compliance uses the following criteria:

1. Does the ranking or award disclose the criteria on which the rating was based.
2. Does the ranking or award validate the appropriateness of advertising the rating (e.g. the Supervised Person knows that it has been the subject of numerous client complaints relating to the rating category or in areas not included in the survey).
3. Does the Supervised Person advertise any favorable rating without also disclosing any unfavorable rating.
4. Does the advertisement state or imply that the Supervised Person was the top-rated person in a category when it was not rated first in that category.

5. Does the advertisement clearly and prominently disclose the category for which the rating was calculated, or designation determined, the number surveyed in that category, and the percentage that received that rating or designation.
6. Does the advertisement disclose that the rating is not representative of any one client's experience because the rating reflects an average of all, or a sample of all, of the experiences of clients.
7. Does the advertisement disclose that the rating is not indicative of the future performance of the Supervised Person.
8. Does the advertisement disclose prominently who created and conducted the survey and that the Supervised Person paid a fee to participate in the survey.

Supervised Person's third-party rankings or awards are required to be approved by Compliance prior to their use in any materials.

Designations and Credentials.

The Firm allows the use of approved designations and credentials by its Supervised Persons. For a designation or credential to be approved by Compliance, it must satisfy the following criteria.

1. The credential/designation requires an examination and that the Supervised Person successfully passes the examination.
2. The credential/designation requires at least 6 hours of CE credits per year (or an average of at least 6 hours if the CE credit requirements are over a period of more than 1-year).
3. The credential/designation has a formal complaint process that can be submitted from the www.finra.org site (see link below).
4. A Supervised Person can determine if a credential/designation satisfies the Firm's requirements by using the link below:

   http://www.finra.org/investors/professional-designations

Procedures

1. **Approved Marketing Materials**
   Supervised Persons are required to use marketing materials that have been reviewed and approved by Compliance.
2. **Client Presentations**
   Supervised Persons are required to ensure that all material to be presented in client meetings have been approved by Compliance.
3. **Performance**
   Supervised Persons are required to use actual performance of the client's account when meeting with clients.

All advertising and client presentation materials must be approved by Compliance prior to first use.

12. ELECTRONIC COMMUNICATIONS

Objective

The objective of the Firm's Electronic Communications policy is to ensure that all Supervised Persons, clients, consultants, vendors, or any persons doing business with the Firm use the Firm's electronic resources in a manner that serves the purpose of supporting the Firm's business and policies. It provides a safeguard to the Firm's confidential information, as well as the Firm's clients and Supervised Persons sensitive information. The policy also serves to limit the possibility of damage to and unauthorized access and use of the Firm's systems and data.

Supervisory Responsibility

The CCO is responsible for ensuring that the Firm's electronic communications systems are being utilized solely for authorized business purposes in conformance with applicable laws, rules and regulations, including all policy and procedures set forth herein. As used in this policy, the term "**electronic communications**" includes, but is not necessarily limited to, business communications made through any of the following media:

1. Voice Communications that includes voicemail, telephones, and mobile telephone devices and related protocols.
2. Mobile computing devices (iPads, tablets, etc.).
3. Electronic mail that includes e-mail, instant messaging, and text messaging.
4. Facsimile that includes e-fax services.
5. The internet and intranet, including the Web, file transfer protocols ("**FTP**"), remote host access, etc.
6. Video teleconferencing.
7. Peripheral devices (iPods, USB and thumb drives, etc.).

Policies

The following summarizes the requirements of the Firm's electronic communications policy:

1. The Firm's electronic communications systems are to be used for business purposes only.
2. All electronic communications with clients, regulators, or the public concerning Firm business or Supervised Persons business are permitted only on Firm communications systems, unless prior consent has been given by the CCO.
3. Electronic email is monitored, reviewed, and recorded by the Firm using Smarsh.
4. Only the CCO or a person designated by the CCO are permitted to post anything on the Firm's Web site.
5. Supervised Persons are prohibited from posting any information concerning the Firm, its business, or clients to the internet or third-party system, containing references to the Firm, communications involving investment advice, references to investment-related issues or information or links to any of the aforementioned without the approval from Compliance.
6. Supervised Persons are required to adhere to the following, regardless of media used:
   a. Books and records maintenance requirement (See Books and Records).
   b. Prohibition against the use of testimonials (See Advertising).

c. Implementation of security and protection policies (See Privacy Protection and Information Security Policies—Regulation S-P and Written Information Security Policy--WISP).
d. Written supervisory policies.
e. The Firm's Code of Ethics.

Electronic Delivery of Information

Supervised Person's ability and freedom to use the Firm's media is limited as follows:

1. No right to privacy when using the Firm's media and that any information stored, processed, or accessed on the Firm's systems is not private and subject to review by the Firm.
2. Prohibited from sending, displaying or storing any material in any electronic format that violates any policy of the Firm.

Supervised Persons are required to have the word "Confidential" in the subject line when sending an email that contains personal or confidential information of a client. The email must be sent using the Firm's email address provided by the Firm or a Firm approved DBA email address.

Review

The CCO reviews the Firm's use of electronic communications on an annual basis to ensure the following:

1. **Notice.** That electronic notifications to clients are sent in a timely manner and are adequate to properly convey the message.
2. **Access.** That clients who are provided with information electronically are also given access to the same information as would be available to them in paper form.
3. **Security.** That precaution is taken to ensure the integrity, confidentiality, and security of information sent through electronic means and that such precautions have been tailored to the medium used.

Advertising and Sales Literature

Where an electronic medium is used to disseminate advertisements for the Firm's services or other information that is not subject to a delivery requirement, it is subject to the same requirements that apply to such communications made in paper form, and as established in the Firm's policy on Advertising.

Policy Regarding Any Firm Electronic Communication

The Firm's electronic communication policies and procedures include the following:

1. The Firm's Electronic Communications Policy is communicated to all Supervised Persons and any changes in this policy are promptly communicated.
2. Electronic communications records are maintained and arranged for easy access and retrieval to provide true and complete copies with appropriate backup and separate storage for the required periods.

3. Electronic communications are maintained in electronic format and are readily accessible at any time by for a period of five (5) years.

Text Messaging Policy

Supervised Persons are prohibited from using text messaging to communicate to clients.

Standards for Internet and E-mail Communications

Supervised Persons are required to comply with all applicable international, federal, state, and local laws. Electronic communications through the Firm's systems are the property of the Firm and the Firm reserves the right to monitor, audit, record, or otherwise retain electronic communications at any time for appropriate business usage, standards and compliance with this policy, applicable laws and regulations. Supervised Persons that violate these standards can result in written sanctions, monetary penalties, or loss of position. Any questions regarding these, or any policies or procedures should be directed to Compliance.

The following guidelines apply to all Supervised Persons:

1. Required to provide email policies and procedures that include encryption capabilities if using a Firm approved DBA email.
2. Required to use their redhawkwa.com or Firm approved DBA email address for all business-related electronic communications.
3. Required to have the word "Confidential" in the subject line when sending personal or confidential client information. The Firm's electronic communication system encrypts the email if the word "Confidential" is in the subject line and the redhawkwa.com or Firm approved DBA email address is used.
4. Required to contain the most recent and valid information available.
5. Required to delete immediately any communications received with inappropriate content.
6. Prohibited from disseminating proprietary information, unless approved by the Firm.
7. Prohibited from copying or transmitting software or other materials protected by copyright law.
8. Prohibited from sending client's personal and sensitive information to or from their personal email.
9. Required to safeguard access to computers, telephones, and other electronic communications systems. Required to keep passwords in a secure location (either physical or electronic) and change frequently.
10. Required to preserve electronic communications sent and received according to Firm and regulatory requirements.
11. Prohibited from communications with the public unless authorized by the Firm.

Email Policy

The Firm treats email and other electronic communications as written communications and that such communications must always be of a professional nature. The Firm's policy covers electronic communications for the Firm, to or from clients, and any personal email communications within the Firm. Supervised Persons are prohibited from using the Firm's email and any other electronic systems for personal use. Supervised Persons that are using

a Firm approved DBA email, must provide the Firm access to their email server and email policies and procedures that include the encryption capabilities. (See also the Social Media and Blogging Policy).

Supervised Persons are required to understand and follow the Firm's email policy with respect to their individual email communications.

Social Media and Blogging Policy

The Firm allows Supervised Persons to maintain social media accounts consisting of LinkedIn, Twitter, and Facebook, subject to the following policies:

1. Input and maintain their existing social media accounts on Smarsh, which is the Firm's social media monitoring system.
2. Notify Compliance in writing of any new social media accounts or blogs they want to create.
3. On an annual basis, sign an attestation that all social media accounts used during the prior year have been previously reported to Compliance and if one or more are no longer in use, a statement to that effect.
4. Cease using social media in connection with the Firm or its clients when the Supervised Person is no longer associated with the Firm.
5. Ensure that any third-party employed to manage social media must comply with the Firm's policies and procedures.

Social media policies are like the Firm's pre-existing considerations with respect to its advertising policies under 206(4)-1. The Firm requires Supervised Persons when using social media to:

1. Prohibit posting or linking to comments or content that violates copyright laws, is harassing, offensive, defamatory, indecent, or misrepresents the stated policies, practices, performance returns of investment strategies provided by the Firm.
2. Be honest and consistent with professional comments provided to clients while providing advisory services or in presentations.
3. Prohibit comments that are in retaliation to negative posts or comments received. If applicable, contact Compliance to address any issues that are directly related to client issues identified in such posts.
4. Prohibit the acceptance of third-party testimonials or recommendations.
5. Go into the social media site and following the steps to block from view any previously accepted testimonials that can't be deleted. Failure to reject or block previously accepted testimonials is subject to the Firm placing restrictions on future social media usage or possible disciplinary actions.
6. If possible, prohibit the use of the "like" feature on social media sites of others or from re-tweeting materials. If possible, disable the "like" button on the site or blog and remove any instances where someone indicated liking material on these sites as soon as possible.
7. Protect the client's privacy on the social media site by prohibiting the use of a client's identification information including, but not limited to, client name, picture, address, finances, accounting holdings, or any other information specific to a client.

8. Prohibit from using Facebook Chat for business related communication.
9. Prohibit from providing legal or tax opinions or making specific investment recommendations on the social media site.
10. Prohibit from making any negative references about the Firm on the social media site, or from making any misrepresentation as to the title, responsibilities, or function with the Firm.
11. Prohibit from using superlatives, exaggeration, or anything that might suggest a guaranteed return or guaranteed successful results.
12. Prohibit the use of industry jargon and prepare any post so that any person can clearly understand.
13. Prohibit the use of charts, graphs, formulas, or other tools on the social media site that are used in determining which securities to buy or sell or when to do so.
14. Required to follow standard performance guidelines in presenting performance.
15. Prohibit offering reports, services, or analysis labeled as free on the social media site or blog unless it is in fact free with no further obligation or commitment.
16. Prohibit from discussing or disclosing any material non-public information.
17. Prohibit from discussing or disclosing the proprietary information, intellectual property interests, or other trade secrets on the social media site.
18. Required to use appropriate disclosures as to business affiliations, relevant conflicts of interest, and correctly attribute ownership of any comments, statements or quotes to the originator.
19. Required that posts as advertisements cannot have any untrue statement of material fact or otherwise be false or misleading.

Licensing

Supervised Persons are prohibited from using the Firm's electronic communications systems to attempt to affect any transaction in securities, or to render investment advisory services for compensation in any state in which the Firm is not properly notice filed.

Books and Records

The Firm captures, stores, and monitors any social media content that is linked to the Smarsh system for a minimum of five (5) years.

Supervisory Policies

The Firm monitors the social media activity using the Smarsh system. Should inappropriate comments or materials be found on a Supervised Person's social media site, action taken by the Firm is dependent on the results of the investigation and can include:

1. Remedial training on the Firm's advertising and social media policies.
2. Prohibiting from any future use of the social media site.
3. Suspension or termination.

13. CODE OF ETHICS

General Principles

The Firm's Code of Ethics sets forth the standards of conduct expected from Supervised Persons and address personal trading, gifts, the use of inside information, and other situations where there is a possibility for conflicts of interest.

The Firm's Code of Ethics is designed for Supervised Persons to:

1. Protect the Firm's clients by deterring misconduct.
2. Understand the Firm's expectations and the laws governing their conduct.
3. Understand that they are in a position of trust and must always act with complete propriety.
4. Protect the reputation of the Firm.
5. Prevent unauthorized trading in client or their own accounts.
6. Guard against violation of the securities laws.
7. Establish procedures to follow so that the Firm can determine they are complying with the Firm's ethical principles.

Supervised Persons are required to adhere to the following specific fiduciary obligations when dealing with clients:

1. The duty to have a reasonable, independent basis for the investment advice provided;
2. The duty to ensure that investment advice meets the client's individual objectives, needs, and circumstances; and
3. A duty to be loyal to clients.

Scope of the Code of Ethics

Honesty, integrity, and professionalism are hallmarks of the Firm. The Firm maintains the highest standards of ethics and conduct in all its business relationships. This Code of Ethics covers a wide range of business practices and procedures and applies to all Supervised Persons when conducting the business and affairs of the Firm.

The activities of Supervised Persons are required to adhere to the following general principles:

1. Honest and ethical conduct is maintained in all client transactions and such conduct is in a manner that is consistent with the Firm's Code of Ethics, thus avoiding or appropriately addressing any actual or potential conflict of interest or any abuse of their position of trust and responsibility.
2. Prohibited from taking inappropriate advantage of their positions with a client or the Firm.
3. Responsible to maintain the confidentiality of the information concerning the identity of securities holdings and financial circumstances of all clients.
4. Ensure independence in the investment decision-making process.

5. Failure to comply with this Code of Ethics can result in disciplinary action, including the termination of employment by the Firm.

Persons Covered by the Code of Ethics

All Supervised Persons are required to comply with the Firm's Code of Ethics. Any questions as to whether an individual is required to comply with the Firm's Code of Ethics should be directed to Compliance.

Securities Covered by the Code of Ethics

"**Reportable Security"** or collectively **"Reportable Securities**" typically means any stock, bond, future, investment contract, or any other instrument that is considered a security under the Advisers Act. A Reportable Security is very broad and includes investments not ordinarily thought of as securities, including, but not limited to:

1. Options on securities, indexes, and currencies.
2. Limited partnership interests.
3. Foreign unit trusts and foreign mutual funds.
4. Private investment funds, hedge funds, and investment clubs.

Reportable Securities that are excluded from the reporting requirements of Rule 204A-1 include the following:

1. Direct obligations of the U.S. government.
2. Banker's acceptances, bank certificates of deposit, commercial paper and high-quality short-term debt obligations, including repurchase agreements.
3. Shares issued by money market funds.
4. Shares of open-end mutual funds that are registered under the Investment Company Act.
5. Shares issued by unit investment trusts that are invested exclusively in one or more open-end funds, none of which are funds advised or sub-advised by the Firm.

Standards of Business Conduct

Pursuant to Rule 204A-1, the Firm requires a standard of business conduct for its Supervised Persons. This section sets forth those standards.

Compliance with Laws and Regulations

All Supervised Persons are required to comply with applicable federal and state securities laws. When a purchase or sale of a security by a client, Supervised Persons are prohibited from:

1. Defrauding such client in any manner.
2. Misleading such client, including making a statement that omits material facts.
3. Engaging in any act which operates or would operate as fraud or deceit upon such client.
4. Engaging in any manipulative practice with respect to such client.

Conflicts of Interest

Supervised Persons are required to act in a fiduciary capacity and have an affirmative duty of care, loyalty, honesty, and good faith to act in the best interests of its clients. With this

duty, Supervised Persons are to avoid conflicts of interest or are required to fully disclose all material facts concerning any conflict that does arise with respect to any client. A "**conflict of interest**" occurs when a Supervised Person's private interests is inconsistent with the interests of the client and/or the Firm. Additionally, Supervised Persons are required to avoid situations that have even the appearance of conflict or impropriety.

Conflicts among Client Interests.
Conflicts of interest arise when the Supervised Person has reason to favor the interests of one client over another client (e.g., larger accounts over smaller accounts, accounts compensated by performance fees over accounts not so compensated, accounts in which the Supervised Person has made material personal investments, or accounts of close friends or relatives of Supervised Persons). The Firm prohibits Supervised Persons from inappropriate favoritism of one client over another client that would constitute a breach of fiduciary duty.

Competing with Client Trades.
The Firm prohibits Supervised Persons from using knowledge about pending or currently considered securities transactions for clients to profit personally, directly or indirectly, as a result of such transactions, including purchasing or selling such securities.

Insider Trading
Supervised Persons are prohibited from trading, either personally or on behalf of others, while in possession of material, nonpublic information. Additionally, Supervised Persons are prohibited from communicating material nonpublic information to others in violation of the law.

1. ***Penalties.*** Should a Supervised Person violate the Firm's insider trading policies and procedures, potential penalties can include, but are not limited to, civil injunctions, permanent bars from employment in the securities industry, civil penalties up to three times the profits made, or losses avoided, criminal fines, and jail sentences.
2. ***Material Nonpublic Information.*** The SEC's position is that the term "**material nonpublic information**" relates not only to issuers, but also to the Firm's securities recommendations and client securities holdings and transactions.

Personal Securities Transactions
Supervised Persons are required to strictly comply with the Firm's policies and procedures regarding personal securities transactions outside of the Firm. The following procedures are designed to assist the Firm in detecting and preventing abusive sales practices.

1. ***Trading Alongside Clients.*** Supervised Persons are prohibited from purchasing or selling any security prior to a transaction being implemented for a client account unless it is approved by Compliance.
2. ***Initial Public Offerings – Prohibition.*** Supervised Persons are prohibited from directly or indirectly acquiring beneficial ownership[1] of any security in an initial public offering.

[1] The term "beneficial ownership" as used in this Code of Ethics is to be interpreted by reference to Rule 16a-1 under the U.S. Securities Exchange Act of 1934, as amended. Under the Rule, a person is generally deemed to have beneficial ownership of securities if the person, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, has

3. ***Limited or Private Offerings – Pre-Clearance.*** Supervised Persons are prohibited from directly or indirectly acquiring beneficial ownership of any security in a limited or private offering, without the specific, advance written approval from Compliance. In determining whether to grant permission for such limited or private placement, Compliance shall consider, among other things, whether such offering should be reserved for a client and whether such transaction is being offered to the Supervised Person because of their position with the Firm.

Any Supervised Person who has received such permission shall be required to disclose such an investment when participating in any subsequent consideration of such security for purchase or sale by client of the Firm, and that the decision to purchase or sell such security shall be made by persons with no personal, direct or indirect, interest in the security.

If a Supervised Person has any question as to whether a possible investment is an initial public offering or a limited or private placement, they should consult with Compliance.

1. ***48-hour Blackout Period.*** With the exception of exchange traded funds ("**ETF**"s) and exchange traded notes ("**ETN**"s), Supervised Persons are prohibited from purchasing or selling any Reportable Security within 48 hours immediately before or after a calendar day on which any client account managed by the Firm purchases or sells that Reportable Security (or any closely related security, such as an option or a related convertible or exchangeable security), unless the Supervised Person had no actual knowledge that the reportable security (or any closely related security) was being considered for purchase or sale for any client account. If any such transaction occurs, the Firm requires any profits from the transaction to be disgorged for donation by the Firm to charity. The total blackout period is four (4) calendar days (two [2] calendar days before and two [2] calendar days after). Supervised Persons can trade alongside clients, if the transactions are at a price equal to or inferior to the price obtained by clients.
2. ***Restricted List.*** Compliance maintains a list of restricted securities and Supervised Persons are prohibited from purchasing or selling those securities while they are on the restricted list without prior written approval of Compliance.
3. ***Prohibition on Participation in Investment Clubs.*** Supervised Persons are prohibited from participating in or making investments with or through any investment club or similar association or entity except with the specific, advance written approval of Compliance. If a Supervised Person has any doubt or uncertainty as to whether an association or entity is an investment club, they should contact Compliance before becoming involved with the association or entity.

---

or shares a direct or indirect pecuniary interest in the securities. The term "pecuniary interest" means the opportunity, directly or indirectly, to profit or share in any profit derived from a transaction in the subject securities.

Notwithstanding the fact that a Supervised Person has not purchased a security for their own account or the account of an immediate family member, if at any time a Supervised Person becomes aware that they have become a beneficial owner of a security in an initial public, limited or private offering (e.g., a purchase made by an immediate family member, which is any relative by blood or marriage living in the Supervised Person's household), the Supervised Person shall promptly report such interest to Compliance who shall determine the appropriate action, if any.

Supervised Persons are prohibited from directly or indirectly advising or causing any immediate family member (i.e., any relative by blood or marriage living in the Supervised Person's household) to engage in conduct the Supervised Person is prohibited from engaging in under the Firm's Code of Ethics.

If a Supervised Person determines within 48 hours immediately before or after they have purchased or sold for their own account a Reportable Security that was not, to the Supervised Person's knowledge, then under consideration for purchase by any client account, the Supervised Person is required to put the clients' interests first and promptly make the investment recommendation or decision in the clients' interest, rather than delaying the recommendation or decision for clients until after the 48 hours following the day of the transaction for the Supervised Person's own account to avoid a possible conflict with the blackout provisions of this Code of Ethics.

Gifts and Entertainment

Supervised Persons are prohibited from accepting gifts, favors, entertainment, special accommodations, or other things of material value that influences their decision-making or make them feel obligated to do business with a person or company. Supervised Persons are prohibited from offering gifts, favors, entertainment, or other things of value that would be viewed as overly generous or aimed at influencing decision-making or making a client feel obligated to do business with the Firm or the Supervised Person.

1. ***Gifts.*** Supervised Persons are prohibited from receiving any gift, service, or other thing of more than de Minimis value from any person or entity that does business with or on behalf of the Firm. Supervised Persons are prohibited from giving or offering any gift of more than de Minimis value to existing clients, prospective clients, or any entity that does business with or on behalf of the Firm without pre-approval by Compliance. Gifts other than cash given in connection with special occasions (e.g., promotions, deaths, births, retirements, weddings), of reasonable value are permissible. Supervised Persons are required to maintain a gift log and to submit the log to Compliance on a quarterly basis.
2. ***Cash.*** Supervised Persons are prohibited from accepting cash gifts or cash equivalents to or from a client, prospective client, or any entity that does business with or on behalf of the Firm. This includes cash equivalents such as gift certificates, bonds, securities, or other items that can be readily converted to cash.
3. ***Entertainment.*** Supervised Persons are prohibited from providing or accepting extravagant or excessive entertainment to or from a client, prospective client, or any person or entity that does or seeks to do business with or on behalf of the Firm. Supervised Persons are prohibited from providing or accepting a business entertainment event, such as dinner, a sporting event, golf outings, etc. provided that such activities involve no more than customary amenities.

Confidentiality

Supervised Persons are required to exercise care in maintaining the confidentiality of any confidential information, except where disclosure is authorized or legally mandated.

Confidential information includes non-public information, the identity of security holdings, and financial circumstances of clients.

1. ***Firm Duties*.** The Firm keeps all information about clients and former clients in strict confidence. This includes the client's identity (unless the client consents), the client's financial circumstances, the client's security holdings, and advice furnished to the client by the Firm or its vendors.
2. ***Supervised Persons' Duties***. Supervised Persons are prohibited from disclosing to persons outside the Firm any material nonpublic information about any client, the securities investments made by the Firm on behalf of the client, information about contemplated securities transactions, or information regarding the Firm's trading strategies, except as required to perform a securities transaction on behalf of a client or for other legitimate business purposes.
3. ***Internal Walls*.** Supervised Persons are prohibited from disclosing nonpublic information concerning clients or securities transactions to any other person within the Firm, except as required for legitimate business purposes.
4. ***Physical Security***. Supervised Persons are required to lock files containing material nonpublic information when not being used or accessed and access to computer files containing such information is restricted to certain permitted persons with unique passwords.
5. ***Regulation S-P*.** Supervised Persons are required to comply with the Firm's privacy policy. Regulation S-P covers only a subset of the Firm's confidentiality standards and applies only to natural persons and only to personal information. The Firm's fiduciary duty to keep client information confidential extends to all the Firm's clients and information, including, but not limited to corporations, limited liability organizations, trusts and estates.

Service of Board of Directors

Supervised Persons must receive written approval from Compliance before serving on a Board of a publicly traded company. Supervised Persons serving as a Director on a Board of a publicly traded company are prohibited from participating in the process of making investment decisions on behalf of clients which involve the subject company, or in any other respect if making such a decision would create the illusion of, or an actual conflict of interest.

Other Outside Activities

Supervised Persons are required to report all outside business activities upon employment and these outside activities are reviewed and approved by Compliance. Supervised Persons are required to receive approval from Compliance for any new outside business activity before engaging in the activity. Supervised Persons are required to receive written approval from Compliance on all outside business activities on an annual basis.

1. ***Executorships.*** Supervised Persons can accept executorships for certain business considerations and family relationships, and it is necessary for the Supervised Person to have written authorization from Compliance to act as an executor. All such existing or prospective relationships should be reported in writing to Compliance**.**

2. ***Custodianships and Powers of Attorney.*** Supervised Persons can accept custodianships and powers of Attorney for minors or other members of the immediate family. These are considered as automatically authorized and do not require approval from Compliance. Supervised Persons must receive approval of Compliance for all other custodianships and entrustment with a Power of Attorney to execute securities transactions on behalf of another.
3. ***Insurance Agents.*** Supervised Persons can act as agents appointed with various life, long-term care, or other insurance companies. Supervised persons can receive commissions, trails, or other compensation from the respective product sponsors and/or as a result of effecting insurance transactions for clients. Clients have the right to purchase insurance products away from the Firm. At all times the Firm and Supervised Persons are to act in the client's best interest and act as a fiduciary in carrying out services provided to the client.
4. ***Disclosure.*** Supervised Persons are required to disclose in writing, any personal interest that might present a conflict of interest or harm the reputation of the Firm.
5. ***Trustees.*** Supervised Persons are prohibited from acting as a trustee except in situations where there is a clear prior and personal relationship. All such existing or prospective relationships should be approved by Compliance.

Marketing and Promotional Activities

Supervised Persons are required to ensure that all oral and written statements, including those made to clients, prospective clients, their representatives, or the media, must be professional, accurate, balanced, and not misleading in any way.

Open Investment Platform ("OIP") Compliance Procedures

General Policy

IARs that are approved for the OIP by Compliance can buy and sell securities on behalf of clients ("**OIP IAR**" or collectively **"OIP IARs**"). OIP IARs are required to provide the following:

1. An investment philosophy document that describes how they are going to manage the investments for their clients. At a minimum, the investment philosophy includes the following:
   a. The objective of the portfolio.
   b. Types of securities that are allowed.
   c. How Best Execution is achieved.
   d. Any tactical or active management processes or policies. These must include how the investments are selected, monitored, and replaced.
2. A personal Investment Policy Statement ("**IPS**") or similar document that is approved by the Firm. The IPS, or similar document that is approved by the Firm, is required to be signed by the client and OIP IAR and must include the client's risk tolerance, retirement goals, time horizon, and a comparison of their current portfolio versus the proposed portfolio.

3. Submit an explanation in writing when changes are made to the investments and an explanation of the changes.
4. Submit documentation of periodic reviews with the client.

Compliance Procedures

Personal Securities Transaction Procedures and Reporting

General Policy/ Pre-clearance

The Firm allows Supervised Persons to buy or sell securities for their personal accounts, subject to the pre-clearance requirements and the prohibitions listed above. Supervised Persons are required to send duplicate statements of their personal accounts to Compliance. Supervised Persons are required pre-clearance for all securities on the Firm's restricted list and Supervised Persons are required to notify Compliance about the purchase or sale of all Reportable Securities, except the following:

1. Purchases or sales over which they have no direct or indirect influence or control;
2. Purchases or sales pursuant to an automatic investment plan;
3. Purchases effected upon exercise of rights issued by an issuer pro rata to all holders of a class of its securities, to the extent such rights were acquired from such issuers, and sales of such rights so acquired;
4. Acquisition of securities through stock dividends, dividend reinvestments, stock splits, reverse stock splits, mergers, consolidations, spin-offs, and other similar corporate reorganizations or distributions generally applicable to all holders of the same class of securities;
5. Open-end investment company shares;
6. Certain closed-end index funds;
7. Unit investment trusts;
8. ETFs and ETNs that are based on a broad-based securities index;
9. Futures and options on currencies or on a broad-based securities index;
10. Assignment of options or exercise of an option at expiration; or
11. Trading alongside clients and receiving the same price as clients.

Any violation, of the aforementioned, can require the Supervised Person to obtain preclearance on all Reportable Securities going forward.

Pre-Clearance Procedures.

The pre-clearance requirements and associated procedures are designed to identify any prohibition or limitation applicable to a proposed investment. Supervised Persons are required to adhere to the following pre-clearance procedures:

1. Submit to Compliance detailed information about the proposed transaction and any additional information.
2. Submit all information before the proposed transaction.
3. Receive an authorization or denial of the transaction by Compliance.
4. Store documentation of the transaction, the approval/denial of and rationale supporting the decision shall be maintained for at least five (5) years after the end of the fiscal year in which the approval/denial was issued.

Compliance can deny or revoke a pre-clearance request for any reason. In no event is pre-clearance granted for any transaction if the Firm has a buy or sell order pending for that same security or a closely related security (such as an option relating to that security, or a related convertible or exchangeable security). Furthermore, in no event is pre-clearance granted for any transaction if the purchase or sale of such security is inconsistent with the purposes of this Code of Ethics and Advisers Act. If approved by Compliance, pre-clearance is valid only for the day on which it is granted and the following one (1) business day.

Reporting Requirements

Supervised Persons are required to submit to Compliance a report of all holdings in Reportable Securities which the Supervised Person has a direct or indirect beneficial ownership as defined by Rule 204A-1, within 10 days of becoming a Supervised Person and thereafter on an annual basis.

For the purposes of personal securities reporting requirements, a Supervised Person's holdings include the holdings of a Supervised Person's immediate family (including any relative by blood or marriage living in the Supervised Person's household), and holdings in any account in which the Supervised Person has direct or indirect beneficial ownership, such as a trust.

The holdings report must include:

1. The title and exchange ticker symbol or CUSIP number, type of security, number of shares, and principal amount (if applicable) of each reportable security in which the Supervised Person has any direct or indirect beneficial ownership.
2. The name of any broker-dealer or bank with which the Supervised Person maintains an account in which any securities are held for the Supervised Person's direct or indirect benefit.
3. The date the report was submitted.
4. The specific account numbers or identifiers in the holdings report.

Quarterly Transaction Reports

Supervised Persons are required to submit to Compliance duplicate statements that include all transactions no later than 30 days after the end of each month. Supervised Persons are required to submit to Compliance duplicate statements for all immediate family members (including any relative by blood or marriage living in their household). Supervised Persons are required to submit duplicate statements to Compliance for any account in which they have a direct or indirect beneficial ownership, such as a trust.

The duplicate statements must include the:

1. Date of the transaction, the title and as applicable the exchange ticker symbol or CUSIP number, interest rate and maturity date, the number of shares, and principal amount of each reportable security involved.
2. Type of the transaction (e.g., purchase or sale).

3. Price of the security at which the transaction was affected.
4. Name of the broker-dealer or bank with or through which the transaction was affected.
5. Date of the statement.

Confidentiality of Reports.
All duplicate statements provided by Supervised Persons concerning their personal transactions and holdings are maintained in confidence, except to the extent necessary to implement and enforce the provisions of the Code of Ethics or to comply with requests for information from government agencies.

Reporting Exemptions.
Supervised Persons are not required to submit duplicate statements: (a) with respect to securities held in accounts over which they have no direct or indirect influence or control; (b) with respect to transactions effected pursuant to an automatic investment plan, including dividend reinvestment plans.

Duplicate Brokerage Confirmations and Statements
Supervised Persons are required to disclose the financial institutions where their assets are held. Supervised Persons are required to direct their financial institutions to provide Compliance duplicate copies of statements that include transactions of all personal securities. Supervised Persons are required to submit duplicate statements in lieu of submitting holdings and transaction reports, provided that all required information is contained in those duplicate statements.

Monitoring of Personal Securities Transactions
Compliance reviews Supervised Persons' personal securities transactions and holdings reports on a monthly basis. The Firm follows these procedures:
1. Compliance reviews and monitors personal securities transactions and trading patterns of Supervised Persons.
2. If Compliance becomes aware of potential violations, a written report explaining the potential violations and the supporting documents is provided to the CCO.

Compliance is required to follow these steps when reviewing personal securities holdings and transactions reports:
1. Assess whether the Supervised Person has followed required internal procedures, such as pre-clearance.
2. Compare personal trading to any restricted lists.
3. Assess whether the Supervised Person is trading for their own account in the same securities the Firm is trading for clients.

Certification of Compliance
1. **Initial Certification.** Supervised Persons are required to certify in writing that they have: (a) received, read, and understand the amendments to the Code of Ethics; (b) read

and understand all provisions of the Code of Ethics; and (c) agreed to comply with the terms of the Code of Ethics.

2. **Acknowledgement of Amendments.** Supervised Persons are required to submit written acknowledgement that they have received, read, and understand amendments to the Code of Ethics as provided by the Firm.
3. **Annual Certification.** Supervised Persons are required to certify that they have read, understand, and complied with the Code of Ethics. In addition, Supervised Persons are required to annually certify that they have submitted the reports required by the Firm and have not engaged in any prohibited conduct. If a Supervised Person is unable to make such representation, they are required to report any violations to Compliance.

Recordkeeping

The Firm maintains the following records in a readily accessible place:

1. A copy of each Code of Ethics that has been in effect at any time during the past five (5) years.
2. A record of any violation of the Code of Ethics and any action taken as a result of such violation for five (5) years from the end of the fiscal year in which the violation occurred.
3. A record of all written acknowledgements of receipt of the Code of Ethics and amendments for each person who is currently, or within the past five (5) years was, a Supervised Person.
4. Holdings and transaction reports made pursuant to the Code of Ethics, including duplicate statements.
5. A list of the names of person who are currently, or within the past five (5) years were, Supervised Persons
6. A record of any decision, and supporting reasons for approving, the acquisition of securities by a Supervised Person in private or limited offerings for at least five (5) years after the end of the fiscal year in which approval was granted.

Form ADV Disclosure

The Firm includes in Form ADV Part 2A, a summary of the Firm's Code of Ethics and states that the Firm provides a copy of the Code of Ethics to any client or prospective client upon request.

Administration and Enforcement of the Code of Ethics

Training and Education

The Supervised Person is responsible for reading, understanding, and abiding by the Firm's Code of Ethics.

1. **Annual Review.** Compliance reviews the adequacy of the Code of Ethics and the effectiveness of its implementation on an annual basis.
2. **Report to Senior Management.** Compliance reports to senior management the annual review of the Code of Ethics and brings material violations to their attention.
3. **Reporting Violations.** Supervised Persons are required to report violations of the Firm's Code of Ethics promptly to Compliance.

4. **Confidentiality**. All reports of violations are treated confidentially to the extent permitted by laws and investigated promptly and appropriately.
5. **Alternate Designee.** The alternate person to whom a Supervised Person can report violations in case the CCO or Designee is involved in the violation. The alternate person is the CEO of the Firm.
6. **Types of Reporting.** Examples of the types of reporting required under this Code of Ethics include: non-compliance with applicable laws, rules, and regulations; fraud or illegal acts involving any aspect of the Firm's business; material misstatements in regulatory filings, internal books and records, client's records or reports; activity that is harmful to clients; and deviations from required controls and procedures that safeguard clients and the Firm.
7. **Apparent Violations.** Supervised Persons are required to report apparent or suspected violations in addition to actual or known violations of the Code of Ethics.
8. **Retaliation.** Retaliation against a Supervised Person who reports a violation is prohibited and constitutes a further violation of the Code of Ethics.

Whistleblower Program

Effective August 12, 2011, The Dodd-Frank Wall Street Reform and Consumer Protection Act (aka the Whistleblower Program) provided the SEC the authority to pay financial rewards to whistleblowers who provide new and timely information about any securities law violation. To be eligible, the whistleblower's information must lead to a successful SEC enforcement action with more than $1,000,000 in monetary sanctions. While the rules incent rather than require prospective whistleblowers to use internal company compliance program, the regulations clarify that the SEC, when considering the amount of an award, considers to what extent (if any) the whistleblower participated in the internal compliance processes of the Firm.

Supervised Persons are required to act in good faith in reporting a complaint or concern and must have reasonable grounds for believing a breach has been made regarding accounting or audit matters, of this Compliance Manual, or of the Firm's Code of Ethics. Supervised Persons who report a malicious allegation known to be false is considered a serious offense and are subject to disciplinary action that can include termination of employment.

Any misconduct by a Supervised Person shall be reported to the CCO. If the misconduct being reported is regarding the CCO, reports shall be made to the CEO. The Firm protects the Supervised Person's identity and won't cause or threaten retaliation of any sort in connection with these reports.

Sanctions

Supervised Persons that violate the Code of Ethics are subject to disciplinary actions that the Firm deems appropriate, including but not limited to, a warning, fines, disgorgement, suspension, demotion, or termination of employment. In addition to sanctions, violations can result in referral to governmental or self-regulatory authorities when appropriate.

Further Information Regarding the Code of Ethics

Should a Supervised Person require additional information about the Code of Ethics or have any other ethics-related questions, they should contact Compliance.

14. PORTFOLIO MANAGEMENT

Portfolio Management and Trading Process

The Firm provides discretionary and non-discretionary portfolio management on a continuous basis. Portfolio management services are not rendered prior to the client entering into a written advisory agreement for services, which is maintained in the client's file. Only designated persons of the Firm and OIP IARs shall exercise discretionary authority over client accounts.

Subject to a grant of discretionary authority, the Firm and OIP IARs, invest and reinvest the securities, cash, or other property held in the client's account in accordance with the client's personal IPS, or similar document approved by the Firm, as identified by the client during initial interviews and information gathering sessions. The Firm and OIP IARs are granted discretion pursuant to authorization provided in the executed agreement for advisory services, which is maintained in the client's file.

When a transaction takes place, the Firm or OIP IAR creates the order and routes it to the trader, who then executes the trade.

Fiduciary Duties Owed to Clients

The Firm and Supervised Persons are required to provide a fiduciary duty to each of its clients. This duty is akin to the "prudent man rule" applicable to a trustee, exercising that degree of care with respect to the client's affairs that a "prudent man" would observe with respect to their own. This duty is particularly evident where the client has given discretionary authority over their account. Consistent with this fiduciary duty, the Firm and Supervised Person is required to communicate any conflicts of interest to the client.

The Firm and Supervised Persons are required to adhere to the following:

1. Avoid all conflicts of interest and potential conflicts of interest.
2. If unavoidable, fully disclose the material facts of every conflict of interest.
3. Exercise the utmost and undivided loyalty to the client in congruence to the Firm's Code of Ethics.
4. Monitor client's circumstances and investments over the course of the relationship.
5. On an annual basis, conduct a formal review with the client and submit the client review to Compliance.
6. Act prudently with the care, skill, and judgment of a fiduciary.
7. Recommend suitable investments that are based on the client's profile that are in their best interest.
8. Obtain Best Execution on client trades.
9. Never engage in front running (*i.e.,* engaging in a trade of a security in the Supervised Person's account in advance of a client's trade in the same security in a manner that is a disadvantage to the client).
10. Treat each client fairly and trade their accounts in an equitable manner.
11. Communicate clearly, accurately, and promptly.

12. Provide accurate information about the total fees and expenses paid by the client.
13. Receive only reasonable gifts, entertainment, and other benefits from service providers, including broker-dealers executing client trades.
14. Maintain a high level of competence regarding investment management knowledge and skills.
15. Ensure that clients are offered or have access to all necessary investment products, funds, and other investment management services that can be tailored to the needs of the client.

Defined Custodian

Client accounts are held in custody by a qualified custodian (the "**Qualified Custodian**") and securities are purchased or sold through the Qualified Custodian's trading platform. Supervised Persons must utilize a Qualified Custodian approved by the Firm in order to participate in asset management services offered by the Firm.

Research Processes

The Firm's research is conducted internally utilizing information obtained from a wide variety of sources. Industry research is used to supplement the Firm's own research efforts and examples of research that are used include Morningstar, TD Ameritrade, Stockopedia, JP Morgan, Goldman Sachs, and Standard & Poors.

Valuation of Securities

The Firm uses information provided by the client's Qualified Custodian as its main pricing source for purposes of valuing client portfolios, both for fee billing and investment performance calculation purposes.

In the rare instance where the Firm believes that the Qualified Custodian is not pricing a security fairly or where a security has halted trading, members of the Firm determines a fair value for that security. The fair value of an account is defined as the amount at which an investment could be exchanged in a current arm's length transaction between willing parties in which the parties each act knowledgeably and prudently. The valuation must be determined using the objective, observable, unadjusted quoted market price for an identical investment in an active market on the measurement date, if available. In the absence of an objective, observable, unadjusted quoted market price for an identical investment in an active market on the measurement date, the valuation must represent the Firm's best estimate of the market value. Fair value must also include accrued income.

Client Review Procedures

IARs are required to conduct a formal review with each client at least annually using the Firm's process and client review documents. Upon completion of the review, IARs must email the completed review form to Compliance.

Account Statements

The Qualified Custodian holding the client's funds and securities send the client a confirmation of every securities transaction and a brokerage statement on a monthly basis.

Additional information relating to the Firm's portfolio management and trading procedures are detailed in the executed advisory agreement located in the specific client file, and in the Form ADV Part 2A.

Compliance with Investment Policies/Profiles, Guidelines and Legal Requirements

The Firm manages each of its client accounts in accordance with the investment policies, restrictions, guidelines, and legal requirements (collectively, "**Investment Restrictions**") applicable to that account.

Sources of Investment Restrictions

There can be several different sources of Investment Restrictions for an account. The principal sources of Investment Restrictions for client accounts typically include the advisory agreement or other instrument under which the account was established, and/or other directions or guidelines established by the client and communicated to the Firm.

In addition, there are various other possible sources of Investment Restrictions for each account, including the Firm's own internal policies (which can further restrict how an account can be managed) and applicable law, which can include, but is not limited to the following:

1. The Advisers Act and interpretations thereunder.
2. The Employee Retirement Income Security Act of 1974 ("**ERISA**"), and related regulations and interpretations of the U.S. Department of Labor (applicable to almost all pension funds, other than governmental and church funds).
3. Other state statutes, regulations, and agency interpretations governing investments of various kinds of governmental assets and pension funds for public employees (these laws differ from state to state and for different categories of accounts even within a single state).
4. State laws, federal laws, and foreign laws, regulating the amount of stock in certain kinds of companies that can be held by accounts owned or managed by a single company (or group of related companies).
5. Insider trading laws.

In addition to laws that limit investments that can be made for a client account, there are other laws that prohibit or limit transactions between a client account and the Firm or its affiliates, and laws that prohibit or limit transactions between certain kinds of client accounts (e.g., ERISA/pension fund clients) and affiliates or other related parties of the client. Many of these laws are the subject of specific policies and procedures covered elsewhere in this Compliance Manual. If a Supervised Person has a question as to whether a particular investment or transaction is legally permissible for an account, they should consult with Compliance before taking any action.

Responsibility for Compliance with Investment Restrictions

Supervised Persons are primarily responsible for compliance with the Investment Restrictions applicable to each account and for the day-to-day management of the account.

Supervised Persons are required to maintain a file for each client account that includes:

1. The advisory agreement.
2. The Qualified Custodian's forms and agreements.
3. A copy of the IPS or similar document approved by the Firm.
4. A copy of any additional instructions, directions, or guidelines established by the client.
5. Copies of governing and offering documents for a pooled vehicle.
6. Copies of any correspondence with the client that can explain the Investment Restrictions for that account.

Supervised Persons are required to understand the Investment Restrictions and investor profile that apply to each account under their management, and to ensure that any transaction made by the Firm on behalf of each such account satisfies both: (1) the Investment Restrictions and/or investor profile applicable to that account and (2) basic standards of suitability and prudence. Supervised Persons are required to continuously review the holdings of their client accounts.

Supervised Persons are required to submit the Investment Restrictions to Compliance and Compliance is responsible for ensuring the information is accurate and complete and signs the document as evidence of their review and approval. The review includes whether the portfolio selected is suitable for the client based on the investor profile unless a written override or special instruction has been signed by the client. Any incomplete documentation is rejected, and no transactions are allowed for such client until complete information is received. This review and acceptance of new clients is done prior to the completion of any initial transaction.

Mutual Fund Share Classes

The Firm only offers institutional share classes (or like share classes) for mutual funds. However, circumstances can be present in which other share classes are in a client's accounts because the client held the shares prior to transferring to the Firm.

Crypto-Asset Policy

IARs are prohibited from providing advisory services regarding investments that are primarily invested in crypto-currencies (e.g. Bitcoin), initial coin offerings, distributed ledger technology, blockchain, or any related products and pooled investment vehicles ("**Crypto-Assets**"). IARs are prohibited from serving in an advisory capacity over any client account that contains any Crypto Asset.

If an IAR is aware that a client is involved in a cryptocurrency and/or block chain trade, they should immediately report this information to Compliance.

Marijuana Policy

The Firm prohibits IARs from conducting business with any person or entity involved with marijuana production, distribution, or other ancillary operations. IARs are prohibited from

establishing new accounts for any of these entities or persons, or maintain any existing accounts discovered after opening. If an IAR is aware of any existing clients involved in the marijuana trade, they should immediately report this information to Compliance.

15. ALTERNATIVE INVESTMENTS

Alternative Investments Overview

Alternative investments represent asset classes outside the realm of traditional stocks, bonds, and cash equivalents and include, among other things, the following:

1. Financial futures/equity futures and options.
2. Leveraged and inverse ETFs.
3. Structured CDs.
4. Hedge funds.
5. Private placements.
6. Non-traded REITS.
7. Direct lending programs.

The Firm requires that all alternative investments engaged by IARs must be approved in writing by the IC prior to use with clients. IARs interested in utilizing the services of an alternative investment that is not currently approved, must be submitted to the IC for review.

Due Diligence of Alternative Investments

The IC performs due diligence on the alternative investment to ensure and understand the structure of the investment, the management of the firm offering the investment, and the risks. This review includes, but is not limited to:

1. Audited financial statements.
2. Offering documents.
3. Background of management.
4. Evaluation of the validity and integrity of the business model and how it fits into its business sector.
5. Determination of the creditworthiness.
6. The assets held by or to be acquired.
7. Review of information available from financial and other publications.
8. Independent verification of management's representations (contact with clients, lenders, vendors, employees, etc.).
9. Review news articles and industry publications regarding the issuer, its market, and competition.
10. Review of internal documents such as operating plans, product literature, corporate records, financial statements, contracts, lists of distributors, and clients.
11. Physical inspection of the facilities.
12. Contact with experts and outside directors.
13. Interview of key personnel or clients.
14. Review of the intended use of proceeds of the investment.

The IC maintains a central file of the information collected during the due diligence. The documents are maintained in accordance with the Firm's books and records procedures and are reviewed and updated periodically. The IC is responsible for documenting the approval of any investment prior to use with any clients.

Training of IARs

The Firm provides education and training to IARs about the alternative investments approved for use with clients. IARs are required to fully understand the investment, its general features, and material risks. Such education and training are documented by Compliance.

Client Review for Use of Alternative Investments

The Firm has implemented specific client guidelines regarding the recommendation of alternative investments with clients. The Firm has determined minimums regarding client's net worth and income that must be met to make any recommendations for use of an alternative investment. All required information gathered from the client is stored in the client's file. IARs are required to ensure that the alternative investment is in the best interest of the client.

IARs are required to consider the following before recommending an alternative investment to a client:

1. Liquidity of the alternative investment.
2. Creditworthiness of the issuer and underlying collateral.
3. Principal and/or income is not guaranteed.
4. Tax consequences or benefits.
5. Costs and fees associated with selling and purchasing.

IARs are required to have the client or prospective client complete an IPS, or similar documents approved by the Firm, outlining their desire for such investments, amount of money to be invested in such opportunities, and a risk profile showing ability to shoulder risk of such investments. IARs are required to have the client complete and sign an acknowledgment form that is designed to identify and have the client acknowledge the material risks associated with the investment (e.g., speculative, illiquid, etc.). IARs are required to forward the completed acknowledgement to Compliance for review.

Disclosure of Risks

IARs are required to maintain documentation of discussions with clients about the use of alternative investments.

Alternative Investment Concentrations

IARs are prohibited from placing more that 10% of a client's investible assets into an alternative investment.

Account Type Considerations

IARs are required to determine if the alternative investment can be held in the account. Some account types do not allow certain types of alternative investments to be purchased or held in the account (based on trust document language, guardianship agreements, retirement plan documents, etc.). Additionally, some account types require financial information to be

considered differently in order to determine the amount of an alternative investment that can be purchased. IARs are required to consider the following:

1. **Trust Accounts:**
   a. Review the trust documents in order to determine if these types of investments can be held in the account.
   b. Irrevocable trusts must use the trust's financial information only. If the trust is established using a tax identification number, the percentage guideline limit for age <70 is used along with the liquid net worth and investment objective.
   c. If the trust is established under a social security number, as opposed to a Tax ID, then the oldest living grantor should be considered for the guideline limits. Personal grantor trusts report annual income, liquid net worth, and net worth, based on the personal financials of the grantor(s).
   d. Assets from a trust established using a tax identification number cannot be commingled with assets of the trustee's personal assets.
2. **UTMA/UGMA/Guardianship/Custodial Accounts:**
   a. The financial information of the adult(s) of the minor(s).
   b. The percentage of the client's liquid net worth is based on the account owner's assets.
   c. For guardianship accounts, review the court documents (if applicable), in order to determine if these types of investments can be held in the account.
3. **Profit Sharing Plans, 401K's, Corporate, and Non-Profit accounts:**
   a. Review the corporate charter documents (if applicable) or any other documents to determine if these types of investments can be held in the account.
   b. Use the entity's financial information.
   c. The percentage must be based on the account's investment objective and financials.
   d. Single participant profit sharing plans and single participant 401k plans should be included in the assets for the individual client/household for whom the account is for the benefit. Review of plan documents should be completed to determine if the plan is a single or multiple participant plan.
4. **Individual Accounts and IRA Accounts:**
   In most cases it is appropriate to use the spouse's information if the client lives in a community property state. However, if the client has a prenuptial agreement then they are not be able to. If the account owner decides to use their spouse's financial information, they must also include that spouse's alternative investment holdings for purposes of calculating allocation percentages.
5. **Joint Accounts:**
   a. Consider the oldest account holder listed on the account to determine age suitability.
   b. Joint accounts must include current and pending alternative investment holdings of all owners whether the additionally disclosed holding is held jointly or individually.

Prospectus/Offering Memorandum Requirement

IARs are required to deliver to the client a copy of the prospectus or offering memorandum for any alternative investment product recommended or sold at the time of the recommendation or sale. IARs are required to fully understand the contents of the fund prospectus/offering memorandum prior to recommending a purchase to clients.

Alternative Investment Exceptions Requests

As a general matter, the Firm does not grant exceptions to firm guidelines and only under a very limited set of facts and circumstances is an exception granted. All exception requests must be presented to Compliance in writing. The information provided to Compliance must include client financial information, beneficiaries, additional insurance policies, health of client, and a compelling reason why client should be allowed to exceed the policy limits. Each request is viewed on a case-by-case basis and can require additional documentation.

Use of Disclosures on Materials

IARs are required to make a full and fair disclosure of all material facts pertaining to alternative investments they solicit or sell. IARs are also required to verify, at the time of purchase, that the client meets all suitability requirements specifically provided in the prospectus or offering memorandum for such security (e.g., minimum annual income and net worth, state regulations, etc.).

Alternative Investment Liquidations and Redemptions

Alternative investment products are meant to be held to maturity through a liquidity event as detailed in the prospectus or offering memorandum. IARs are prohibited from assisting directly in the sale or redemption of an alternative investment unless the client is selling or redeeming back to the general partner (issuer) or if they are accepting a tender offer.

IARs are required to fully inform the client that:

1. Alternative investment units usually sell at a very deep discount to their initial purchase price and can be assessed early redemption fees or contingent deferred sales charges ("**CDSC**").
2. The client is responsible for paying all fees charged by the market maker, issuer, or general partner in relation to the transfer.
3. The transfer process can take longer than eight weeks to be completed.
4. Redemptions are not always possible, and the client should be prepared that they are not be able to liquidate shares.
5. Investing the proceeds of a liquidated alternative investment into a new alternative investment for the purpose of achieving greater distribution should not be recommended, as the distribution rate is not guaranteed and can be reduced or eliminated at the discretion of the sponsor.

Periodically, a client wishes to liquidate some or all their alternative investment holdings. Though there are firms providing secondary markets with services designed to help individuals liquidate certain illiquid alternative investments, IARs are prohibited from assisting clients in effecting transactions with such firms. Additionally, IARs are prohibited from engaging in cross trades for any alternative investment.

16. TRADING AND BROKERAGE POLICY/BEST EXECUTION

Introduction

The Firm recognizes its fiduciary obligation to obtain Best Execution of clients' transactions under the circumstances of the particular transaction. In all cases, the Qualified Custodian selected must be a registered entity with the SEC and a member of FINRA.

The Firm periodically evaluates its relationships with Qualified Custodians to determine Best Execution quality. "**Best Execution**" means that the Qualified Custodian is capable of providing the best qualitative execution of client trade orders under the circumstances, taking into account the full range and quality of the services offered, including the cost of the trade, their financial responsibility, and execution capabilities.

Review of Trade Execution

The Firm monitors and evaluates the execution and performance capabilities of the utilized Qualified Custodian(s). Monitoring methods include, reviews of trade tickets, confirmations and other documentation incidental to trades, and periodic meetings (either in person or via telephone) with various control persons of the Custodian to discuss overall execution.

Disclosure

The Firm discloses the brokerage practices in the Firm's Form ADV Part 2A, including a summary of factors the Firm considers when selecting a Qualified Custodian and determining the reasonableness of their commissions.

Conflicts of Interests

The Firm is sensitive to various conflicts of interest that can arise when selecting a Qualified Custodian to execute client trades, and where necessary, addresses such conflicts by disclosure.

Trade Processing Procedures

Order Placement

OIP IARs have discretion to trade securities on behalf of their clients' subject to the Firm's Code of Ethics, as described above. IARs that are not approved for the OIP are required to adhere to the following general trade in securities practices:

1. IAR communicates the trade to Operations as follows:
   a. **Portfolio Change.** By completing the Firm's appropriate Portfolio Amendment Agreement and emailing it to Compliance.
   b. **Other Changes for Individual Securities.** By sending an email with the trade instructions.
2. Operations enters the trade into the Qualified Custodian's trading platform.
3. Operations organizes the trades and allocates the pro rata share to the applicable accounts. Settlement of all trades is handled by Qualified Custodian.
4. Operations maintains records of executed trades by the Qualified Custodian.

All trading discrepancies, errors, or mistakes shall be brought to the attention of the CCO. Operations maintains a file evidencing the trading discrepancy, error, or mistake, the review conducted by the CCO and any action taken by the CCO with respect thereto. Discrepancies are corrected in conformity with the Firm's Trading Error Procedures.

Aggregation and Allocation of Transactions

The following sets forth the Firm's policies and procedures with respect to the allocation of investment opportunities and trade orders among client accounts and related matters.

1. Operations aggregates transactions if it believes that aggregation is consistent with the duty to seek Best Execution for its clients and is consistent with the disclosures made to clients and terms defined in the client advisory agreement.
2. Operations also makes trades in individual accounts (that are not aggregated with others) so that it addresses that client's unique circumstances.

No client is favored over any other client, and each account that participates in an aggregated order participates at the average share price (per Qualified Custodian) for all transactions in that security on a given business day.

Allocation of Investment Opportunities

Operations aggregates client trades providing that the following conditions are met:

1. The Firm's policy for the aggregation of transactions is fully disclosed to existing clients in the advisory agreement.
2. The Firm does not aggregate transactions unless it believes that aggregation is consistent with its duty to seek the Best Execution (which includes the duty to seek best price) for the client and is consistent with the terms of its advisory agreement with the client for which trades are being aggregated.
3. No client is favored over any other client; each client that participates in an aggregated order participates at the average share price for all our transactions in each security on a given business day, with transaction costs based on each client's participation in the transaction.
4. If the aggregated order is filled in its entirety, it is allocated among clients in an equitable manner.
5. If the order is partially filled, it is allocated to all accounts in the aggregated order. This means that all accounts will receive a partial allocation until all orders are filled.
6. Notwithstanding the foregoing, the order can be allocated on a basis different from that specified if all client accounts receive fair and equitable treatment and the reason for difference of allocation is explained in writing and is reviewed by the CCO. The Firm's books and records separately reflects, for each client account, the orders of which aggregated, the securities held by, and bought for that account.
7. The Firm receives no additional compensation or remuneration of any kind as a result of the proposed aggregation.
8. Individual advice and treatment are accorded to each client.

Whether and to what extent an account participates in an allocation is based on several considerations, including among others, the account's investment objective, policies and

restrictions, its availability of cash balances, tax considerations, and whether the account already has enough holdings of similar securities. Based on these and any other relevant considerations, and except as noted below, each account is generally given the opportunity to participate in potential investments, which fall within that account's investment objective and policy restrictions, on a pro-rata basis based on the relative asset size of the account.

Aggregated Executions

When orders are aggregated, each participating account receives the weighted average price for all transactions in a particular security effected to fill such orders on a given business day, and transaction costs are shared pro rata based upon each account's participation in the transaction. Operations is responsible for oversight and enforcement of this policy.

Compliance Monitoring and Reporting

Compliance monitors and periodically reviews trading issues including, commissions, trading problems or errors, compliance issues, and procedures.

Principal Transactions with Clients

Supervised Persons are prohibited from engaging in principal transactions with clients. Principal transactions are generally defined as transactions where a Supervised Person, acting as principal for its own account, buys from or sells a security to a client.

Economic Benefits from Securities Transactions

Supervised Persons are prohibited from accepting products or services (other than execution and services from a Qualified Custodians) from financial institutions or a third parties in connection with client securities transactions. Such products or services can be classified as a "**Soft Dollar Benefit**" or "**Other Economic Benefit**."

Soft Dollar Benefits – Definition

Supervised Persons are prohibited from entering any type of Soft Dollar Benefit. A Soft Dollar Benefit is when a Supervised Person enters into a type of arrangement with one or more financial institutions whereby it receives some benefit in exchange for directing client transactions to the financial institution. These benefits can be paid for with what are commonly referred to as "soft dollars," and are referred to as "soft dollar benefits."

Other Economic Benefits

Supervised Persons are prohibited from entering any type of Other Economic Benefit. An Other Economic Benefit is when a Supervised Person receives from a financial institution, without cost, computer software and related systems support, which allows the Supervised Person to better monitor client accounts maintained at that financial institution ("other economic benefit"). The Supervised Person receives the software and related support without cost because it renders advisory services to clients that, in the aggregate, maintain a certain level of assets at that financial institution.

Example of Other Economic Benefits

The following illustrates additional Other Economic Benefits that a Supervised Person can receive:

1. Receipt of duplicate client confirmations and bundled duplicate statements.
2. Access to a trading desk that provides for specialized services.
3. Access to block trading for client trade orders.
4. Access to an electronic communication network for client order entry and account information.
5. Software or other tools in connection with the delivery of advisory services.
6. Travel, meals, entertainment, and admission to educational or due diligence programs.
7. Marketing support including sponsorship of client events.

17. TRADE ERROR PROCEDURES

Introduction

The following procedures provide guidance on how trading errors are handled and to whom issues regarding trading errors or potential trading errors should be directed to ensure that they are handled promptly and appropriately.

Definition of Trade Error

A trading error is a deviation from the applicable standard of care in the placement, execution, or settlement of a trade for a client account. In general, the following types of errors are considered trading errors for the purposes of these procedures if the error resulted from a breach in the duty of care that the Firm and OIP IARs ("**Trader**") owes to the client under the circumstances:

1. The purchase or sale of the wrong security or wrong amount of securities.
2. The over purchase of a security.
3. The purchase or sale of a security in violation of client investment guidelines or other failure to follow specific client directives.
4. Purchase of securities not legally authorized for the client's account.

For purposes of these procedures, the following types of errors are not deemed to be trading errors:

1. Good faith errors in judgment in making investment decisions for clients.
2. Errors caught and corrected before execution.

Policy

An overriding principle in dealing with a trading error made by a Trader (or any other party to the trade other than the client) is that the client never pays for losses resulting from such errors. When the error and responsible party are identified, the Trader works with the Qualified Custodian to correct the trade error. If possible, the trade is broken immediately by the Qualified Custodian and the error is corrected the same day. The Trader works with the Qualified Custodian on making the client's account whole with no loss to the client's account. If there is a loss to the client's account, the Trader works with the Qualified Custodian to reimburse the client's account. Traders are prohibited from varying from these procedures and the Firm can institute written sanctions, monetary penalties or, loss of position, or termination. Any questions regarding error correction, policy or procedures should be directed to the CCO.

Trade Error Notification Procedures

Traders are required to adhere to the following in the event a potential trading error is identified:

1. Alert the CCO immediately.
2. Determine whether a trading error has occurred and the responsible party.
3. Work with the CCO to determine the best course of action to correct the trading error.

4. Once the best course of action is determined, work with the Qualified Custodian to correct the error as soon as possible, that is in the best interest of the client, and in a manner consistent with the Policy outlined above.
5. In the event of a loss, work with the Qualified Custodian to reimburse the account from the Firm's fee or sundry account for the full amount of the loss, including transaction costs.
6. In the event of an erroneous profit, the profit is immediately donated to a charity that has been pre-determined by the Firm and is connected to the Firm's fee or sundry account.
7. The Trader documents the trading error and sends it to the CCO. The documentation is required to include: (1) the date of the trading error, (2) the account(s) involved, (3) the security involved (including CUSIP), (4) a brief description of the error, (5) the amount of the gain or loss, and (6) recommended changes to the policy to prevent the error from occurring in the future.
8. Payments made to clients as a result of trade error correction are recorded in the Firm's accounting records.
9. Only the Firm has the authority to reimburse clients.
10. The CCO determines if a pattern of errors exists that should otherwise be addressed.
11. The Firm maintains a record of all trade error reports for a period of five (5) years.

18. FINANCIAL PLANNING

Introduction

The Firm requires all financial planning activities conducted by Supervised Persons for compensation to be conducted through the Firm. By its general nature, financial planning is a broad term that can or cannot include advice on securities. The financial planning activities available to Supervised Persons include:

1. Retirement income and retirement cash flow planning.
2. Social security optimization planning.
3. Investment policy statement design.
4. Income tax planning.
5. Estate planning.
6. Business and business continuation planning:
    a. 401(k)
    b. 403(b)
    c. SIMPLE
    d. SEP
    e. Cash balance
    f. Defined Benefit
    g. Employee Stock Option Plan ("**ESOP**")
    h. Captive insurance
7. Risk management planning:
    a. Life
    b. Health
    c. Disability
    d. Long-term care
8. Charitable giving and philanthropic planning.

Additional financial planning activities can be offered by Supervised Persons to clients or prospective clients based on their needs and desires. Any financial planning activity that is not identified above, must be approved in writing by Compliance.

Required Agreements

Supervised Persons are required to execute the Firm's Financial Planning Agreement with the client prior to providing the financial planning services

Duties in Providing Financial Planning Services

Supervised Persons are required to conduct financial planning activities in a manner that are consistent as a fiduciary. In meeting such requirements, Supervised Persons are required to have a duty to:

1. Have a reasonable and independent basis for their investment advice.
2. Ensure that their investment advice is suitable to the client's objectives, needs and circumstances.
3. Be loyal to clients as it adheres to the Firm's compliance and Code of Ethics.

Supervised Persons are prohibited from:

1. Employing a device, scheme, or artifice to defraud a client or a prospective client.
2. Engaging in any practice, transaction, or course of business which defrauds or deceives a client or a prospective client.
3. Engaging in fraudulent, manipulative, or deceptive practices.

Recordkeeping

Supervised Persons are required to:

1. Email an electronic copy of the signed Financial Planning Agreement to Compliance.
2. Store a copy of the Financial Planning Agreement.
3. Store a copy of the actual financial plan or documents provided to clients pursuant to providing the financial planning services.
4. Provide Operations and Accounting with the client's name, email, and signed authorization for Accounting to electronically invoice the client.
5. Forward any checks or payments received by the client to the CCO, who will then forward the check to Accounting.

19. WRAP FEE PROGRAM

Introduction

The Firm offers a "**Wrap Fee Program**" defined as "any program under which a client is charged a specified fee or fees not based directly upon transactions in the client's account for advisory services (which can include portfolio management or advice concerning the selection of other investment advisors) and execution of client transactions."

The Firm acts as sponsor for its own Wrap Fee Program and is compensated under this program for organizing or administering the program. Currently, the only professional portfolio manager in the Firm's Wrap Fee Program is Redhawk Wealth Advisors, Inc. The Firm has an Appendix to Part 2A of the Form ADV that is used as the Wrap Fee Program disclosure brochure and is provided to all prospective and current clients. Initial and annual delivery requirements are the same as those required for Form ADV Part 2A. Such brochure is kept current and made available to the SEC and all other regulatory authorities upon request.

For the Wrap Fee Program, the Firm charges accounts an annual advisory fee that is billed monthly in arrears and is based on a percentage of assets under management. The annual advisory fee covers both investment management and financial advisory. The Firm pays for all trading and transaction expenses for the account. The Qualified Custodian provides the client with trade confirmations and monthly brokerage statements.

Under the Wrap Fee Program, the Firm acts in the best interests of its clients and understands that it has a duty to obtain Best Execution. The Firm manages other accounts that are not part of a Wrap Fee Program. The Firm uses block trading to assist in potentially avoiding an adverse effect on the price of a security that could result from simultaneously placing several separate, successive, or competing client trade orders.

Supervised Persons are required to consider whether the Wrap Fee Program is suitable and appropriate for its client prior to entering into such an arrangement. There is no difference between how the Firm manages the Wrap Fee Program accounts and how it manages other accounts.

20. ERISA PLANS

Policy

The Firm acts as an investment manager for advisory clients (typically the plan sponsor of a qualified retirement plan) which are governed by ERISA ("**Covered Plan**" or collectively "**Covered Plans**"). Under certain circumstances, the Firm is treated as giving "investment advice" to a plan or a plan fiduciary for purposes of section 3(21) and 3(38) of ERISA. When giving "investment advice" with respect to a plan, the Firm is treated as a co-fiduciary or a fiduciary under ERISA. As an investment manager and a fiduciary with special responsibilities under ERISA, and as a matter of policy, the Firm acts solely in the interests of the plan participants and beneficiaries. The Firm is required to manage client assets consistent with the "Prudent Man Rule," maintaining any ERISA bonding or fiduciary liability insurance that is required and obtaining written investment guidelines and investment policy statements.

Only the Firm can serve as an ERISA 3(38) investment manager for the Covered Plan. A Supervised Person can serve as an ERISA 3(21) investment advisor for the Covered Plan.

QDIA Regulation

The Department of Labor ("**DOL**") adopted the Qualified Default Investment Alternative ("**QDIA**") Regulation (ERISA Section 404(c)(5)) to provide relief to a plan sponsor from certain fiduciary responsibilities for investments made on behalf of participants or beneficiaries who fail to direct the investment of assets in their individual accounts.

For the plan sponsor to obtain safe harbor relief from fiduciary liability for investment outcomes the assets must be invested in a QDIA as defined in the regulation. While investment products are not specifically identified, the regulation provides for four types of QDIAs:

1. A product with a mix of investments that take into consideration the individual's age or retirement date (e.g., a life cycle or target date fund).
2. An investment services product that allocates contributions among existing plan options to provide an asset mix that takes into consideration the individual's age or retirement date (i.e., a professionally managed account).
3. A product with a mix of investments that considers the characteristics of the group of employees rather than everyone (e.g. a balanced fund).
4. A capital preservation product for only the first 120 days of participation (an option for plan sponsors wishing to simplify administration if employees opt-out of participation before incurring an additional tax).

A QDIA must either be managed by (i) an investment manager, (ii) a plan trustee, (iii) a plan sponsor, or (iv) a committee primarily comprised of employees of the plan sponsor that is a named fiduciary, or it can be an investment company registered under the Investment Company Act of 1940. It is the policy of the Firm that investment advice given by the Firm with respect to Covered Plans concerning default investment options for participants or

beneficiaries ensures that plan fiduciaries wanting to offer a QDIA can do so consistent with the QDIA Regulation.

ERISA Disclosures - 408(b)(2)

Under ERISA section 408(b)(2), covers service providers that are required to provide to the responsible plan fiduciary advance disclosures concerning their services and compensation ("**Covered Service Provider**" or collectively "**Covered Service Providers**"). This regulation amends a prohibited transaction rule under ERISA and the Internal Revenue Code. That rule states that it is a prohibited transaction for a Covered Plan to enter into an arrangement with a Covered Service Provider unless the arrangement is reasonable, and the compensation being received by the Covered Service Provider is reasonable. The final regulation imposes specific disclosure requirements intended to enable the plan's responsible plan fiduciary to determine whether a Covered Service Provider arrangement is reasonable and identifies potential conflicts of interest.

Investment Advice – Participants and Beneficiaries

Supervised Persons acting as a fiduciary are permitted to render investment advice to participants and receive compensation for such advice pursuant to an "eligible investment advice arrangement." Such arrangement must provide for either:

1. Level compensation, meaning that any direct or indirect compensation received by the fiduciary cannot vary depending on the participant's selection of a particular investment option, or
2. A computer model, which an independent expert must certify as being unbiased.

Investment Advice – IRAs

Under ERISA, fiduciaries are held to duties of loyalty and prudence (among other duties) under Section 404(a) of ERISA and are subject to the prohibited transaction rules of Section 406 of ERISA and Section 4975 of the Code. The Final Regulation applies to Supervised Persons giving "investment advice" to IRAs or IRA holders. The prohibited transaction rules would prevent a Supervised Person with any conflict of interest from giving fiduciary "investment advice" to an IRA or IRA holder without a Prohibited Transaction Exemption.

The Firm requires that all Supervised Persons serve in the best interest of the retirement client and adhere to and comply with the following Impartial Conduct Standards that include:

1. **Best Interest of the Client**: Supervised Persons are required to provide investment advice that is, at the time made, in the client's best interest**.** This means that the to the extent investment advice is provided to the client for their retirement account, the investment advice reflects the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent person acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims, based on the investment objectives, risk tolerance, financial circumstances, and the retirement needs, without regard to the financial or other interests of the Supervised Person.

2. **Reasonable Compensation**: Supervised Persons are prohibited from providing investment advice that causes them to receive compensation, directly or indirectly, that is in excess of reasonable compensation within the meaning of ERISA Section 408(b)(2) and/or Code Section 4975(d)(2). This means that the compensation cannot be excessive as measured by the market value of the services they provide to the client and their retirement accounts.
3. **Non-Misleading Statements**: Supervised Persons are required to ensure that all communications to the client in connection with investment advice regarding the client's retirement accounts, which include the recommended transaction, the fees incurred in connection with the transaction, the compensation received, any material conflicts of interest, and any other information relevant to the investment decision, won't be materially misleading at the time made.
4. **Level Fee Fiduciary**: Supervised Persons are required to act as a level fee fiduciary. A level fee is a fee or compensation that is provided based on a fixed percentage of the value of the assets or a set fee that does not vary with the particular investment recommended, rather than a commission or other transaction-based fee. Supervised Persons are prohibited from receiving any other remunerations (e.g., commissions, 12b–1 fees or revenue sharing), beyond the level fee in connection with advisory services with respect to the Covered Plan or IRA.

Conflicts of Interest - IRAs

Supervised Persons are required to disclose all conflicts of interest to the prospective client before entering into an advisory agreement.

1. **The Conflict of Interest**

   The DOL asserts that there is a clear and substantial conflict of interest when a Supervised Person recommends that a participant roll money out of a plan into a fee-based account that generates ongoing fees for the Supervised Person that they would not otherwise receive, even if the fees going-forward do not vary with the assets recommended or invested. Similarly, the prohibited transaction rules could be implicated by a recommendation to switch from a low activity commission-based account to an account that charges a fixed percentage of assets under management on an ongoing basis.
2. **Conditions of the Streamlined Conditions**
   a. **Status.** Supervised Persons are required to adhere to a level fee fiduciary, as described above.
   b. **Disclosure.** Supervised Persons are required to provide the client a written statement of its fiduciary status prior to or at the same time as the execution of the recommended transaction.
   c. **Comply with Impartial Conduct Standards**. Supervised Persons are required to comply with the Impartial Conduct Standards listed above.
3. **Documentation**

   Supervised Persons are required to document the specific reason or reasons why the recommendation is in the best interest of the client by completing the Firm's Rollover Checklist.

a. Supervised Persons are required to document the rollover from a Covered Plan to an IRA, the documentation must include:
    i. Consideration of the client's alternatives to a rollover, including leaving the money in their current employer's plan, if permitted.
    ii. Considering the fees and expenses associated with both the plan and the IRA.
    iii. Whether the employer pays for some or all of plan's administrative expenses.
    iv. The different levels of services and investments available under each option.
b. Supervised Persons are required to document the rollover from another IRA or to switch from a commission-based account to a level fee arrangement, the documentation must include:
    i. The services that are provided for the fee.

Responsibility

The CCO is responsible for implementing and monitoring of the Firm's ERISA policy, practices, disclosures, and recordkeeping.

21. OPENING ACCOUNTS FOR SENIOR INVESTORS

Objective

On Jan. 24, 2018 the United States House of Representatives passed the Senior Safe Act. The Senior Safe Act (referred to as "the Act," formerly H.R. 3758) encourages financial services firms to train employees to spot elder abuse, while granting limited immunity to individuals at financial institutions who report such abuse to law enforcement or regulators in accordance with the Act.

In response to the Senior Safe Act, the Firm has adopted the following best practices when dealing with senior clients age 65 or older ("**Senior**" or collectively "**Seniors**").

Definition of Trusted Contact

A "**Trusted Contact Person**" is intended to be a resource for client accounts, protecting assets, and responding to possible financial exploitation of any vulnerable client particularly Seniors.

Clients who name a Trusted Contact Person with the Firm provide written authorization to reveal certain information about the client and their accounts to the Trusted Contact Person. While the Trusted Contact Person cannot direct transactions in the account, they can learn certain sensitive information about account balances, holdings and beneficiaries as well as other information related to the senior's health, estate planning (e.g., individuals designated with legal powers, trustees, guardianship, executor, etc.). The Firm is further authorized by the client to use discretion when providing the necessary disclosures to the Trusted Contact Person.

Process

Supervised Persons are required to ask for information about a Trusted Contact Person when a Senior client engages with the Firm for advisory services or for existing accounts. The Senior client isn't required to provide the name of a Trusted Contact Person. A Trusted Contact Person must be a person over age 18; however, the amendment does not include any other requirements, for example: joint account holders, trustees, and persons having powers of attorney can be named as a Trusted Contact Person.

Supervised Persons are required to consider the following when serving Senior clients:

1. Encourage the Senior client to identify a Trusted Contact Person and obtain permission to contact that person in the event there is an issue or an event that requires clarification (such as the Senior client suffers diminished mental capacity in the future).
2. Document if the Senior client refuses to identify a contact person and place it in the Senior client's file.
3. Indicate "retired" on the Qualified Custodian's new account form to assist in evaluating the Senior client's status as someone potentially withdrawing from investments vs. accumulating assets.

4. Obtain "lifestyle" information such as when the Senior client plans to retire, if not already retired; how much money is needed after retirement; whether there are prospects for future employment; whether a dependent is supported by the Senior client; other expenses, including healthcare expenses, anticipated by the Senior client; the existence of a will and financial power of attorney. These should all be collected from the Senior client when they first become a client and during periodic client review meetings.

The absence of the name of or contact information for a Trusted Contact Person shall not prevent the Firm from opening or maintaining an account for a Senior client, provided that the Supervised Person makes reasonable efforts to obtain the name of and contact information for a Trusted Contact Person.

Diminished Mental Capacity

Supervised Persons are required to take the following steps to protect the Senior client if their behavior suggests reduced capacity:

1. Contact the Trusted Contact Person, if applicable.
2. Discuss the situation with the Senior client and determine if family members should be contacted.
3. If applicable, raise the issue with the Senior client's family members and determine if the Senior client has given power of attorney to another person.
4. Document meetings, conversations, and other exchanges with relatives about the situation and store in the Senior client's file.
5. Document communications with the Senior client about investments.
6. Decide not to continue doing business with the Senior client.
7. Contact Compliance with questions about a proper course of action.

Potential Indication of Elder Financial Exploitation

Supervised Persons, through monitoring transaction activity that is not consistent with expected behavior, can become aware of persons or entities perpetrating illicit activity against a Senior client. Additionally, Supervised Persons can become aware of such scams through their direct interactions with Senior clients who are being financially exploited. Such activity can include erratic or unusual transactions, changes in account patterns, or suspicions interaction with a Senior client's caregiver.

22. COMPLAINTS

Supervisory Responsibility

The CCO is responsible for ensuring that all written and electronically transmitted client complaints are handled in accordance with all applicable laws, rules, and regulations and in keeping with the provisions of this Section.

Definition

The Firm defines a "**complaint**" as any statement (whether delivered written, orally, or electronically) made by a client, or any person acting on behalf of a client, alleging a grievance involving the activities of a Supervised Person in connection with its management of the client's account.

Handling of Client Complaints

1. The Firm takes client complaints seriously and Compliance promptly initiates a review of the factual circumstances surrounding any complaint that has been received.
2. Supervised Persons are required to notify Compliance immediately upon receipt of a written, oral, or electronic client complaint and provide all information and documentation in their possession relating to such complaint.
3. Supervised Persons are required to cooperate fully with Compliance and with regulatory authorities in the investigation of any client complaint.
4. Compliance maintains a separate file for all written, oral, and electronically transmitted client complaints to include the following information:
    1. Identification of each complaint.
    2. The date each complaint was received.
    3. Identification of the Supervised Persons servicing the account.
    4. A detailed description of the complaint.
    5. Copies of all correspondence involving the complaint.
    6. The written report of the action taken with respect to the complaint.

23. CORRESPONDENCE

Introduction

Supervised Persons are required to use discretion in communicating information to clients and prospective clients. This policy applies to all communications used with existing or prospective clients, including information available in electronic form such as on a web site. Supervised Persons are required to ensure all client communications are presented fairly, are balanced, and are not misleading.

Definition

Correspondence includes incoming and outgoing written and other communications to clients or prospective clients, regardless of the method of transmission (mail, facsimile, personal delivery, courier services, electronic mail, etc.). Correspondence also includes seminars, panel presentations, speeches, and other types of information originated by a Supervised Person and provided to one or more clients or prospective clients. Interactive conversations such as personal meetings, telephone conversations (other than scripted sales calls), and posting to and in "chat rooms are generally considered correspondence. Advertising, sales literature, and market letters are not included in this definition of correspondence; rather, they are covered in the Advertising section of this Compliance Manual.

Outgoing Correspondence

1. **Responsibility.** Compliance is responsible for ensuring that all outgoing correspondence regarding client investments is approved, reviewed, and retained in Compliance with the Firm's guidelines and the applicable laws, rules, and regulations. Supervised Persons who transmit any correspondence regarding client investments are required to ensure that a copy of the correspondence is reviewed by Compliance. Compliance annotates the review and/or approval of all correspondence and stores such correspondence in the Supervised Person's file.
2. **General Guidelines for Outgoing Correspondence**
   Supervised Persons are required to adhere to the following for outgoing correspondence:
   a. Required to send and receive all correspondence at such locations and through such channels as are designated by the Firm. No Firm-related correspondence of any kind, including electronic correspondence, can be sent or received through a non-business computer without written approval of Compliance.
   b. Required to be truthful and in good taste.
   c. Prohibited from containing exaggerated or outrageous language.
   d. Prohibited from containing projections or predictions except when in accordance with the Firm's policies regarding advertising.
   e. Prohibited from photocopying and distributing copyrighted material in violation of copyright laws.
   f. Required to ensure that the use of letterhead and other official stationery is limited to business related matters.

g. Prohibited from sending materials to anyone outside the Firm that are marked "For Internal Use" or with words of similar effect.
h. Prohibited from making any statements or supplying any information about a security that is the subject of a securities offering other than the information contained in offering materials that have been approved for such offering. Violations of this policy can subject the Supervised person to severe civil and, in some cases, criminal liability.

Incoming Correspondence

1. **General.**
   a. All incoming correspondence is opened and reviewed.
   b. Correspondence subject to this policy includes letters, facsimiles, courier deliveries, and other forms of communication, including, but not limited to, communications marked "personal," "confidential," or words to this effect.
2. **Procedures.**
   a. Client complaints are immediately forwarded to Compliance.
   b. Original client correspondence is retained in the client's file.

Records

Supervised Persons are required to maintain written correspondence at the principal place of business for a period of five (5) years or longer if required by applicable SEC or state regulations. Electronic correspondence is retained in the format in which it was received.

Personal Mail

Supervised Persons are prohibited from having personal mail sent to their place of business. All mail received at the place of business is subject to the Firm's incoming mail review policies.

24. REGULATION S-P - PRIVACY PROTECTION & INFORMATION SECURITY POLICIES

Introduction

Regulation S-P ("**Reg S-P**") requires an RIA to adopt and implement policies and procedures that are reasonably designed to protect the confidentiality of nonpublic personal records. Reg S-P applies to "client" records, meaning records regarding individuals, families, or households. The Firm is committed to protecting the confidentiality of all nonpublic information regarding its clients and Supervised Persons ("**Nonpublic Personal Information**").

Supervised Persons are required to provide clients with notices describing the Firm's privacy policies and procedures. Supervised Persons are required to deliver the privacy notices to all new clients upon entering into an advisory agreement. The Firm delivers the privacy notices to clients annually thereafter, if applicable. The Firm does not distribute its privacy policy to companies or to individuals representing legal entities (Reg S-P does not require the distribution of privacy notices to these entities).

Scope of Policy

This Privacy Policy covers the Firm's practices and applies to all Nonpublic Personal Information of current and former clients.

Overview of the Guidelines for Protecting Client Information

Supervised Persons are required to adhere to the following standards:

1. Ensure the security and confidentiality of client records and information.
2. Protect against any anticipated threats or hazards to the security or integrity of client records and information.
3. Protect against unauthorized access to or use of client records or information that could result in substantial harm or inconvenience to any client.

Supervised Persons Responsibility

Supervised Persons are:

1. Required to protect the Nonpublic Personal Information of clients collected by and/or in their possession.
2. Prohibited from disclosing or using Nonpublic Personal Information of clients without the prior written consent of the client.
3. Required to ensure that the Nonpublic Personal Information of clients is shared only with others that is consistent with the Firm's Privacy Notice and the procedures contained in this Reg S-P policy.
4. Required to ensure that access to the Nonpublic Personal Information of clients is limited as provided in the Privacy Notice and this Reg S-P policy.
5. Prohibited from selling Nonpublic Personal Information of clients.
6. Prohibited from disseminating proprietary information and/or Nonpublic Personal Information and sensitive client data. This includes sending client Nonpublic Personal

Information to personal emails and unauthorized downloading of confidential client information to a thumb or zip drive.

7. Contact Compliance with questions concerning the collection, sharing, or accessing, Nonpublic Personal Information of clients.

Supervised Persons that do not adhere to these policies is cause for disciplinary action, up to and including termination of employment for cause and referral to appropriate civil and criminal legal authorities.

Information Practices

Supervised Persons collect Nonpublic Personal Information about clients from various sources. These sources and examples of the types of information collected include:

1. Product and service applications or other forms, such as client surveys, agreements, etc., typically including, but not limited to, name, address, age, social security number, taxpayer ID number, assets, and income.
2. Past transactions, which can include, but are not limited to, account balances, types of transactions, and investments.
3. Other third-party sources.

Disclosure of Information to Non-affiliated Third Parties – "Do Not Share" Policy

The Firm has a "Do Not Share" Privacy Policy. Supervised Persons are prohibited from disclosing any Nonpublic Personal Information about clients or former clients to non-affiliated third parties. Additionally, Supervised Persons are prohibited from sharing credit-related information, such as income, total wealth, and credit information with non-affiliated third parties.

Types of Permitted Disclosures – The Exceptions

Reg S-P contains several exceptions which permit the Firm to disclose client information (the "**Exceptions**"). For example, the Firm is permitted under certain circumstances to provide information to non-affiliated third parties to perform services on the Firm's behalf. In addition, there are several "ordinary course" exceptions which allow the Firm to disclose information that is necessary to effect, administer, or enforce a transaction that a client has requested or authorized. A more detailed description of these Exceptions is set forth below.

1. **Service Providers.** The Firm has relationships with non-affiliated third parties that require it to share client information for the third-party to carry out services for the Firm. These non-affiliated third parties represent situations where the Firm offer products or services jointly with another financial institution, thereby requiring the Firm to disclose client information to that third-party. Every non-affiliated third-party that falls under this Exception has entered into an agreement that includes the confidentiality provisions required by Reg S-P, which ensure that each such non-affiliated third-party uses and re-discloses client Nonpublic Personal Information only for the purpose(s) for which it was originally disclosed. Some of the non-affiliated service providers that fall under this type of relationship include:
   a. Riskalyze

b. Orion
c. E-valuator
d. Smarsh

2. **Processing and Servicing Transactions**. The Firm also shares information when it is necessary to effect, administer, or enforce a transaction for the client or pursuant to written client requests. In this context, "Necessary to effect, administer, or enforce a transaction" means that the disclosure is required, or is a usual, appropriate, or acceptable method:
   a. To carry out the transaction or the product or service of which the transaction is a part, and record, service, or maintain the client's account in the ordinary course of providing the financial service or financial product.
   b. To administer or service benefits or claims relating to the transaction or the product or service of which it is a part.
   c. To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the client or the client's agent.
   d. To accrue or recognize incentives or bonuses associated with the transaction that are provided by the Firm or any other party.

Some of the non-affiliated service providers that fall under this type of relationship include the following Qualified Custodians:

a. TD Ameritrade
b. Schwab
c. Fidelity
d. Interactive Brokers

3. **Sharing as Permitted or Required by Law.** The Firm discloses information to non-affiliated third parties as required or allowed by law. This includes, for example, disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, an audit or examination, or the sale of an account to another financial institution. The Firm takes the appropriate steps to ensure that it is sharing client data only within the exceptions noted above. The Firm achieves this by understanding and limiting how the Firm shares data with its clients, their agents, service providers, parties related to transactions in the ordinary course, or joint marketers.

Provision of Opt Out

The Firm operates under a "Do Not Share" policy and therefore does not need to provide the right for its clients to opt out of sharing with non-affiliated third parties. If the Firm's information sharing practices change in the future, the Firm can implement an opt-out policy and procedure and make the appropriate disclosures to clients.

Safeguarding of Client Records and Information

The Firm has implemented internal controls and procedures designed to maintain accurate records concerning clients' personal information. The Firm's clients have the right to contact the Firm if they believe that Firm records contain inaccurate, incomplete, or stale information about them. Operations responds in a timely manner to requests to correct information. To protect this information, the Firm maintains appropriate security measures for its computer and information systems, including the use of passwords and firewalls. (See also ***Written Information Security Policy*** below.)

The Firm has a formal Document Management Process and uses shredding machines, locks, and other appropriate physical security measure to safeguard client information stored in paper format. Supervised Persons are required to secure client information in locked cabinets when the office is closed.

Security Standards

The Firm maintains physical, electronic, and procedural safeguards to protect the integrity and confidentiality of client information. Internally, The Firm limits access to clients' Nonpublic Personal Information to those employees who need to know such information in order to provide products and services to clients. Supervised Persons are required to understand and comply with these information principles.

Privacy Notice

The Firm has developed a Privacy Notice, as required under Reg S-P, to be delivered to clients initially by Supervised Persons. The notice discloses the Firm's information collection and sharing practices and other required information and has been formatted and drafted to be clear and conspicuous. The notice is revised as necessary any time information practices change. The Firm notifies clients of any change to its Privacy Notice on an annual basis.

Initial Privacy Notice

Supervised Persons are required to provide the Firm's Privacy Notice to all new clients at the time when the client relationship is established, specifically, upon the execution of the advisory agreement.

Revised Privacy Notice

The Firm delivers its Privacy Notice to all clients if there is a change in the Firm's collection, sharing or security practices. This is delivered on an annual basis if applicable.

Regulation S-ID – Identity Theft Red Flag Rules Applicable to Investment Advisors

It is the policy of the Firm to protect client accounts from identity theft and to comply with the SEC's Red Flags Rule. The Firm has developed and implemented an Identity Theft Protection Policy ("**ITPP**"), which is appropriate to the size and complexity, as well as the nature and scope of the Firm's activities. The ITPP addresses:

1. Identifying relevant identity theft red flags.

2. Detecting those red flags when they appear.
3. Responding appropriately to any reed flags that are detected to prevent and mitigate identity theft.
4. Updating the ITPP periodically to reflect changes in risks.

Compliance reviews the ITPP periodically to ensure it accounts for changes both in regulations and in the Firm's business.

Identifying Relevant Red Flags

The Firm assesses these risk factors to identify relevant identity theft red flags:

1. The types of accounts offered.
2. Any previous experience with identity theft.

The Firm also considers red flags from the following five categories of the SEC's Red Flags Rule:

1. Alerts, notifications, or warnings from a credit reporting agency.
2. Suspicious documents.
3. Suspicious personal identifying information.
4. Suspicious account activity.
5. Notices from other sources.

Detecting Red Flags

The Firm reviews its client accounts, how they are opened and maintained, and how to detect red flags that have occurred in working with its clients. The Firm's detection process of identifying the red flags are based on its methods of gathering information about clients, working with its Qualified Custodians for discrepancies in client information, verifying clients who access their accounts, and monitoring transactions and change of address requests.

Procedures to Prevent and Mitigate Identity Theft

When the Firm is notified of a red flag, or the detection procedures shows evidence of a red flag, the Firm takes the steps outlined below, as appropriate to the type and seriousness of the threat:

1. ***Applicants:*** For red flags raised by someone attempting to become a client.
    a. **Review the Application**
    Compliance collects the applicant's information for the Firm's records and Qualified Custodian paperwork (*e.g.*, name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
    b. **Seek Additional Verification from Custodian or Office of Foreign Assets Control ("OFAC")**
    Compliance verifies the person's identity through non-documentary methods, including:
        i. Contacting the Qualified Custodian for verification check.
        ii. Checking references with other affiliated financial institutions.

iii. Obtaining a financial statement.

c. **Deny the Application**
Compliance abstains from engaging with the client if it finds that the applicant is using an identity other than their own.

d. **Report**
Compliance reports the applicant to the appropriate local and state law enforcement if it finds that the applicant is using an identity other than their own.

2. ***Seekers:*** For red flags raised by someone seeking to access an existing client's account:

a. **Watch**
Compliance monitors, limits, or suspends activity in the account until the situation is resolved.

b. **Check with the Clients**
Compliance collaborates with the Supervised Person of the account. The Supervised Person contacts the clients using its existing contact information on file for the client, describe what it found, and verify with the client that there has been an attempt at identify theft.

c. **Heightened Risk**
Compliance determines if there is a particular reason that makes it easier for an intruder to seek access, such as a client's lost wallet, mail theft, a data security incident, or the client's giving account information to an imposter pretending to represent the Firm or to a fraudulent website.

d. **Collect Incident Information**
If available, Compliance collects the following additional information:

1. D
ates and times of activity.
2. S
ecurities involved (name and symbol).
3. D
etails of trades or unexecuted orders.
4. D
etails of any wire transfer activity.
5. C
lient's accounts affected by the activity, including name and account number.
6. W
hether the clients are reimbursed and by whom.

e. **Report**
Compliance reports any unauthorized account access to the Qualified Custodian, appropriate local law enforcement, and state law enforcement. Compliance also reports the findings to the SEC, state regulatory authorities, such as the state securities commission, and the custodian.

f. **Notification**
Compliance prepares any specific notice to clients or other required notice under state law if it determines that personally identifiable information has been accessed that results in a foreseeable risk for identity theft.

g. **Assist the Clients**

Supervised Persons works with the clients to minimize the impact of identity theft by taking the following actions, as applicable:

i. Offering to change the password, security codes, or other ways to access the threatened account.
ii. Offering to close the account.
iii. Instructing the clients to go to the FTC Identity Theft Website to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

Qualified Custodian and Other Service Providers

All client accounts are held at a Qualified Custodian. The Firm has a process to confirm that the Qualified Custodian and any other service provider that performs activities in connection with client accounts, especially other service providers that are not otherwise regulated, comply with reasonable policies and procedures designed to detect, prevent, and mitigate identity theft. The Firm requires that its service providers, by contract, have such policies and procedures and either report the red flags that can arise in the performance of the service providers' activities to the Firm or take appropriate steps of their own to prevent or mitigate the identify theft or both.

Updates and Annual Review

Compliance updates this plan whenever there is a material change. The grid below, provides the Red Flags Rule categories and examples of potential red flags. These examples are neither an exhaustive nor a mandatory checklist, but a way to help Compliance evaluate relevant red flags in the context of its business.

Red Flag	Detecting the Red Flag
Category: Suspicious Documents	
1. Identification documents look altered or forged.	The Supervised Person contacts Compliance and Compliance scrutinizes identification presented in person to make sure it is not altered or forged.
2. Other information on the identification does not match other information the Supervised person has on file for the presenter. (Example: the original account application, signature card or a recent check).	The Supervised Person contacts Compliance and Compliance ensures that the identification presented and other information on file from the account, such as [describe the information] are consistent.
3. The application looks like it has been altered, forged or torn up and reassembled.	The Supervised Person contacts Compliance and Compliance scrutinizes each application to make sure it is not altered, forged, or torn up and reassembled.

Red Flag	Detecting the Red Flag
Category: Suspicious Personal Identifying Information	
4. Inconsistencies exist between the personal identifying information presented and information the Supervised person knows about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.	The Supervised Person contacts Compliance and Compliance checks personal identifying information presented to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File.
5. Inconsistencies exist in the personal identifying information that the client provides the Supervised Person, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	The Supervised Person contacts Compliance and Compliance checks personal identifying information provided to make sure that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables.
6. Personal identifying information presented has been used on an account the Supervised Person knows was fraudulent, such as the address or phone number provided on the application is the same as the address or phone number on a fraudulent application.	The Supervised Person contacts Compliance and Compliance compares the information presented with addresses and phone numbers on accounts or applications it found or were reported were fraudulent.
7. Personal identifying information presented is a type commonly associated with fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid or is for a pager or answering service.	The Supervised Person contacts Compliance and Compliance validates the information presented when opening an account to ensure they are real and not for a mail drop or a prison and calls the phone numbers given to ensure they are valid and not for pagers or answering services.
8. The SSN presented was used by someone else opening an account or other clients.	The Supervised Person contacts Compliance and Compliance compares the SSNs presented to see if they were given by others opening accounts or other clients.
9. The address or telephone number presented has been used or is like those used by many other people opening accounts or other clients.	The Supervised Person contacts Compliance and Compliance compares address and telephone number information to see if they were used by other applicants and clients.
10. The person opening the account, or the client omits required personal identifying information on an application or in response to notification that the application is incomplete.	The Supervised Person tracks when applicants or clients have not responded to requests for required information and follow up with the applicants or clients to determine why they have not responded.
11. Inconsistencies exist between the personal identifying information that is presented and what is on file.	The Supervised Person contacts Compliance and Compliance verifies key items from the data presented with information on file.
Category: Unusual Use of, or Suspicious Activity Related to, the Account	

Red Flag	Detecting the Red Flag
12. Soon after the Qualified Custodian receives a change of address request for an account, the Qualified Custodian receives a request for new or additional access means (such as debit cards or checks) or authorized users for the account.	The Qualified Custodian verifies change of address requests by sending a notice of the change to both the new and old addresses so the clients learn of any unauthorized changes and can notify us.
13. An account develops new patterns of activity, such as nonpayment inconsistent with prior history; a material increases in the use of available credit; or a material change in spending patterns or electronic fund transfers.	The Supervised Person contacts Compliance and Compliance reviews accounts on a monthly basis and checks for suspicious new patterns of activity such as nonpayment, a large increase in credit use, or a big change in spending or electronic fund transfers.
14. Mail that the Supervised Person sends to a client is returned repeatedly as undeliverable even though the account remains active.	The Supervised Person contacts Compliance and Compliance notes any returned mail for an account and immediately check the account's activity.
15. The Supervised Person is notified that a client is not getting their paper account statements.	The Supervised Person records on the account any report that the client is not receiving paper statements and immediately investigate them. They contact Compliance if necessary.
16. The Supervised Person is notified that there are unauthorized charges or transactions to the account.	The Supervised Person contacts Compliance and Compliance verifies if the notification is legitimate and involves a firm account, and then investigate the report.
Category: Notice from Clients, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with an Account	
17. The Supervised person learns that unauthorized access to a client's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	The Supervised Person contacts the client to learn the details of the unauthorized access to determine if other steps are warranted. They contact Compliance if necessary.

25. WRITTEN INFORMATION SECURITY POLICY ("WISP")

Overview

This policy serves to further provide protection of any and all personal information for clients and shall further identify all procedures to be carried out in the event of a security breach as defined by the Privacy Protection and Information Security Policy above.

The Firm provides adequate protection and confidentiality of all corporate data and all personal information whether held centrally, on local storage media, or remotely to ensure the integrity of all data and configuration controls.

Scope

This policy applies to Supervised Persons, contractors, consultants, and other workers at the Firm ("**Users**"). This policy also applies to all equipment that is owned or leased by the Firm ("**Firm Equipment**"). The policy further applies to all Firm business which includes Firm systems, records that can contain personal information about a current client, whether electronic, paper, computing systems, storage media, laptops, portable devices, and other records ("**Firm Business**"). Firm systems are those systems that the Firm makes available to Users or the Firm uses to support its business and regulatory requirements ("**Firm Systems**") and includes, but is not limited to:

Available to Supervised Persons

1. Microsoft Office 365
2. Orion
3. Riskalyze
4. Redtail
5. FMG Suite
6. Adobe
7. ScheduleOnce
8. Qualified Custodian's systems
9. Other third-party provider systems
10. Social media sites used for business
11. Company web site

Available to Employees of the Firm

1. E-Valuator
2. Smarsh
3. Advisor Armor
4. Firm Plus
5. ScheduleOnce
6. Morningstar
7. Stockopedia
8. SurePayroll
9. QuickBooks

10. Zoom
11. Keeper
12. Docusign
13. FINRA
14. Wistia
15. Camtasia
16. Qualified Custodians systems
17. Other third-party provider systems
18. Social media sites used for business
19. Firm web sites

General Use and Ownership

Any data created by Users on Firm Systems or for Firm Business remains the property of the Firm.

1. All information stored on the Firm's network including email, file systems, and databases are the property of the Firm and Users should have no expectation of privacy for this data.
2. The Firm monitors stored files and internet access (for those Users with Firm Equipment) for the protection of Users, for system performance, maintenance, auditing, security or investigative functions (including evidence of unlawful activity or breaches to the Firm's policy) and to protect itself from potential corporate liability.
3. Compliance monitors all incoming and outgoing emails for compliance purposes.
4. The Firm audits networks and systems on a periodic basis to ensure compliance with this policy.

Network Access

User Identification and Passwords

For Firm Systems, Compliance assigns Users usernames and Compliance requires that Users do not write their usernames down or disclose it to any other individual. Users of a given username are held responsible for all actions performed under use of that username.

For Firm Business, Users are required to change passwords at least every four months (120 days) for any Firm System that contains personal information about a client. Users are required to adhere to the following:

1. Don't reveal a password over the phone.
2. Don't reveal a password in an email message.
3. Don't reveal a password to any individual.
4. Don't talk about a password in front of others.
5. Don't hint at the format of a password (e.g., my street name).
6. Don't reveal a password on questionnaires or security forms.
7. Don't share a password with family members.
8. Don't reveal a password to co-workers.
9. Don't write passwords down and store them anywhere in your office.

10. Don't store passwords on any computer system, including handheld devices, without encryption.

Users are prohibited from choosing passwords that can be easily guessed. Users are prohibited from inserting passwords into email messages or other forms of electronic communication. Users can use a password manager application if the data is encrypted and approved by Compliance. If an account or password is suspected to have been compromised, immediately report the incident to Compliance.

Computer Security

1. **General**
   a. Personal computers ("**PC**" or collectively "**PCs**"), desktop computers, and notebook computers used for Firm Systems or Firm Business are required to be put into "sleep mode" or "shutoff" when left unattended and must be password protected when accessing.
   b. All reasonable precautions must be taken to protect Firm Equipment against damage, loss, and theft. Firm Equipment must not be left unattended in any public place. Damage, loss, or theft must be immediately reported to Compliance.
   c. All computers used for Firm Systems and Firm Business are required to be protected with hard drive encryption that requires a password before booting.
   d. The Firm inventories Firm Equipment on an annual basis.
2. **Software**
   a. It is prohibited for Users to copy, remove, or transfer any software used for Firm Systems or Firm Business to any third-party or non-organizational equipment such as home computers without authorization from Compliance.
   b. It is required that Users only use software that has been approved by the Firm for Firm Business.
   c. It is prohibited for Users to download any executable files (.exe) or software from the internet onto Firm Equipment without authorization from Compliance.
   d. The Firm removes any files or data from Firm Systems it views as offensive or illegal.
   e. The Firm inventories all Firm Systems utilized by Users on an annual basis.
3. **Confidentiality**
   a. It is required that Users store confidential data for Firm Business securely, even when not in use. Files are required to be password-protected.
   b. Computers used for Firm Systems or Firm Business that are to be destroyed are required to have the hard disk "wiped clean" and physically destroyed by a third-party specializing in such activity.

Internet and Email

1. **Internet**
   a. For Firm Business, Users are required to use the internet in a professional, ethical, and lawful manner.
   b. For Firm Business, Users are required to exercise caution when making payments over the internet, as the security of credit card details cannot be guaranteed. The

Firm does not accept any liability for losses arising through the transmission of personal or financial information (e.g. credit card numbers) over the internet.

c. For Firm Business, Users are prohibited from using the same passwords for login to internet websites as they do for Firm Systems.
d. The Firm prevents internet access for Users of Firm Equipment who do not follow its policies.

2. **Email**
   a. For Firm Business, Users are required to use their redhawkwa.com or Firm approved DBA email address.
   b. For Firm Business, Users are required to put the word "Confidential" in the subject line of the email when sending personal and sensitive information. The Firm's email system automatically encrypts emails that have the word "Confidential" in the subject line and are sent via the redhawk.com or Firm approved DBA email address.
   c. For Firm Business, Users are required to inform Compliance when they receive an email which they deem to be inappropriate, offensive, or illegal.
   d. For Firm Business, Users are required to use the Firm's standard email signature with appropriate Firm disclosures. Users are prohibited from including their own logo, designations, and disclaimers to emails, unless approved in writing by Compliance.

Removable and Mobile Media

1. For Firm Business, Users are prohibited from storing sensitive client data on removable media unless pre-approved by Compliance for a specific purpose. If approved by Compliance, the files on the removable media must be password-protected.
2. For Firm Business, Users are required to use Firm-approved email signatures and disclosures when using a mobile device to send or receive emails.
3. For Firm Business, Users are responsible for the security of all mobile devices. The device is required to have password protection and a time-out feature that shuts down the device no more than 30 minutes from last use.
4. For Firm Business, Users are required to have encryption software and anti-virus scanning software on their mobile device.
5. For Firm Business, Users are required to immediately report the loss or theft of a mobile device (for those Users with Firm Equipment) to Compliance.

Remote Access

1. **Wireless Access**
   The Firm reviews all cloud-based software to ensure its security for working remotely via a wireless network. For Firm Business, User email accounts are encrypted for both webmail and desktop software as described above. Data stored by the Firm is only stored on the servers of cloud-based software which use SSL and encryption to protect the data and provide a secure connection. For Firm Business, Users that work remotely are required to access the Firm's server using a virtual private network.
2. **Prevention of Data Loss**
   All computers used for Firm Business are required to have the following security configuration to prevent data loss in the event of theft:

a. Required to be protected with hard drive encryption that requires a password to boot.
b. Required to access documents remotely and not downloaded to the computer.
c. Required to have a password protected screensaver.

3. **Remote Device Protection**
   For Firm Business, Users are required to have anti-virus software configured to automatically download, install, and use the latest virus signatures.
4. **Authentication**
   For Firm Business, Users are required to use two-stage authentication at a minimum for remote access.

Backups of Sensitive Data

For Firm Business, Users are required to:

1. Securely store with either password protection or encryption backup files containing sensitive data.
2. Securely store when not in use, any and all media used for backups of sensitive data.
3. Wipe clean and securely discard backup media when it's rendered unusable.

Third-Party Access

1. Third-Party Access can be defined as "Access to the Firm's IT resources or data to an individual who is not a Supervised Person."
2. Such individuals include:
   a. Software vendor providing technical support.
   b. Contractor or consultant.
   c. Service provider.
   d. An individual providing outsourced services to the Firm requiring access to applications and data.
3. Third-party access is only permitted to facilities and specific tasks as identified and approved by the Firm.

Employee or Equipment Changes

1. Users are required to notify the appropriate "**IT Resource**" (which is defined as the person responsible for overseeing the information technology at the Firm or the IAR's office, as applicable) when moving to a new position or location within the Firm to ensure required network adjustments are made.
2. Users are required to notify the appropriate IT Resource of all staff changes that might affect security. An example of this would be an individual who has access to restricted confidential information and moves to another role where this access is not required.
3. Users are required to notify the appropriate IT Resource to access the computer account of another User who is absent from the office.
4. If a User's employment is terminated, the following steps are required to be taken immediately by the appropriate IT Resource:
5. The User's network account is disabled immediately.
6. The User's cloud-based access is disabled immediately.

7. The User's passwords are changed or deleted immediately.
8. The User's access to Firm Systems are terminated immediately.
9. The User's computer is inspected and prepared for re-distribution and all data saved locally is moved to a separate and secure place on the network.
10. If a User is promoted or demoted, the appropriate IT Resource should be informed of the change immediately in order that network permission levels can be adjusted as required and appropriate for the new role.
11. The appropriate IT Resource must be notified of any employee departure immediately for the IT Resource to ensure their accounts are adjusted as required for compliance with this policy.

Paper Records

1. Any and all paper records that contain personal information are required to be secured in a locked cabinet, drawer or alternate container. Keys, safe codes or combinations are to be kept securely with the appropriate manager and not distributed verbally or electronically to any other individuals.
2. Any records that are used for business purposes and contain personal information that are not to be maintained, are required to be immediately destroyed upon completion of use as required for business purposes. Paper documents are required to be shredded as opposed to simply being discarded in a trash receptacle.
3. Paper records of any kind related to business practices, clients, or affiliates are prohibited from being be removed from the organization without prior authorization.

Fraudulent Email Requests and Compromised Client Email Accounts

Users are prohibited from accepting trade or withdrawal requests from an incoming call without verifying the identity of the client.

Data Security Coordinator

1. The CCO is the primary point of contact for all matters related to this written policy.
2. The CCO maintains documentation in connection with the program including a log of any breach incidents, program revisions, etc.

Training

1. Users have access to the WISP and are required to adhere to it in its entirety.
2. Training is held periodically by the Firm to Users for the understanding of requirements and Firm practices associated with data protection and encryption.
3. All training sessions and updates to the provisions or the Firm's policy are documented.

Risk Analysis

Periodic security checks are performed by a third-party vendor to ensure compliance with the written information security program. Intentional attempts to Users or sensitive information on computers or the network help to ensure that network safeguards for data security are current, effective, and compliant with the requirements.

Enforcement

Any User found to violate this policy is subject to disciplinary action, up to and including termination.

Response to Security Breach

In the event of a suspected or known security breach of personal information, it is required that the steps below are followed:

1. An immediate meeting between the CCO and all involved parties shall be held to determine the root cause and consequence of the incident.
2. The CCO shall contact the affected party immediately to bring the breach to their attention.
3. Depending on the nature of the breach, any and all efforts should be made to recover from the breach (i.e., retrieve sensitive documents from inappropriate recipient, etc.).
4. If applicable, any new safeguards required for prevention of such a breach in the future is put in place as soon as possible.
5. The CCO documents the incident and keep it on record in the WISP log.
6. If disciplinary action is required, the appropriate manager shall act as deemed appropriate, up to and including termination.

26. BUSINESS CONTINUITY and DISASTER RECOVERY PLAN ("BCDRP")

Introduction

This policy outlines the Firm's immediate and long-term contingency planning and recovery process. The purpose of the BCDRP is to provide specific guidelines for the Firm to follow in the event of a failure of any critical business capability. The BCDRP relates to the Firm's ability to resume normal business activities following a disaster. Disasters can come from outside sources, such as terrorist activities and weather-related events, or from personal events such as the death or disability of a key person.

The plan that is included in this manual is a high-level overview and a detailed plan is held by the Firm.

It is required that all Supervised Persons follow the same plan as the Firm.

Purpose

The primary purpose of this plan is to prevent severe and prolonged business interruption or downtime in order to protect clients, Supervised Persons, vendors, service providers, and the Firm. This plan focuses on preparing for a host of natural and man-made disasters to include cyber-attacks.

The proactive part of the plan is the Business Continuity ("**BC**") piece and the Disaster Recovery Plan ("**DRP**") portion is more reactive. Both plans fit together and are updated on an annual basis. The planning is focused on office facilities, computers, data security, and communications.

Business Impact Analysis

The Firm's Business Impact Analysis ("**BIA**") predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios have been identified during the risk assessment. The Firm's operations can also be interrupted by the failure of a supplier of goods or services or delayed deliveries. There are many possible scenarios that were considered.

Identifying and evaluating the impact of disasters provides the basis for investment in recovery strategies as well as investment in prevention and mitigation strategies.

The BIA identifies the operational and financial impacts resulting from the disruption of business functions and processes. Impacts that were considered include:

1. Lost sales and income.
2. Delayed sales or income.
3. Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.).
4. Regulatory fines.
5. Contractual penalties or loss of contractual bonuses.
6. Client dissatisfaction or defection.
7. Delay of new business plans.

8. Timing and duration of disruption.

It is the Firm's position that financial impact risks are mitigated by the insurance it carries and its corporate assets.

Conducting the BIA

The Firm has a BIA questionnaire to survey managers and others within the Firm. The questionnaire surveyed those with detailed knowledge of how the business manufactures its products or provides its services. The Firm asked managers who run critical departments to identify the potential impacts if the business function or process that they are responsible for is interrupted. The BIA also identified the critical business processes and resources needed for the business to continue to function at different levels.

BIA Report

The Firm's BIA report documents the potential impacts resulting from disruption of business functions and processes. Scenarios resulting in significant business interruption have been assessed in terms of financial impact. These costs are then compared with the costs for possible recovery strategies. The BIA report prioritizes the order of events for restoration of the business and the business processes with the greatest operational and financial impacts are restored first.

Possible business disruption scenarios:

1. Physical damage to the office buildings.
2. Damage to or breakdown of machinery, systems, or equipment.
3. Restricted access to a site or building.
4. Interruption of the supply chain including failure of a supplier or disruption of transportation of goods from the supplier.
5. Utility outage (e.g., electrical power outage).
6. Damage to, loss, or corruption of information technology including voice and data communications, servers, computers, operating systems, applications, and data.
7. Absenteeism of essential employees.

Employee, Office Building, and Contents Security & Safety

The Firm has an onsite cloud-based security camera system that can see both entries into the office. The system records any movement to the cloud and is stored for 30 days (each new day of movement over-writes a day of storage). The Firm's building has 24 x 7 security at the main entrance and key card access. Supervised Persons, and vendor files are stored electronically in the cloud. Offsite storage of paper files and documents that are less than 5 years old are secured in a shared storage facility.

If the building lost power, it is conceivable the Firm could be locked out for a period. The building does have a diesel backup generator in case of a power outage. The generator only provides power to selected outlets in the office. If the Firm's building lost power, the Firm does not lose the ability to keep the doors locked and the security camera system continues to run on battery backup for 12 hours.

Cyber Threats

The Firm does possess client data in the form of social security numbers which are in electronic form and in certain Firm Systems. The Firm does not directly receive or store credit card information for clients or Supervised Persons. Payments that are made via credit card are transacted through a third-party electronic billing system and the client enters their credit card information. The Firm does not have access to credit card information.

The Firm has Webroot monitoring on each computer system tied to the Firm's network and Katharion that blocks unwanted corporate spam. The Firm's latest firewall upgrade includes a service that circumvents threats, such as ransomware, from occurring on the Firm's network.

Natural Disasters

The Firm's common natural disasters include the following:

1. Snowstorm - Very common in the state and expected each winter.
2. Lightening - Common in the state and power outages and computer failures have occurred for various reasons over the Firm's history.
3. Flood - Common in the state, however the building has never been impacted.
4. Tornado - Common in the state, however the building has never been impacted.
5. Earthquake - Not common but possible.

Probable Events and Severity Levels

Below are the likely events that could cause anything from short-term down drafts to a longer-term stoppage of the Firm's business and the severity level for each one (1-highest severity to 6-lowest severity):

Event	Severity Level
1. Terrorism	1
2. Food/water outage and/or contamination	1
3. Kidnapping	1
4. Anarchy – government overthrow	1
5. Water damage due to roof leaks, HVAC, fire extinguishment or plumbing issues	2
6. Fire	2
7. Disease outbreak	2
8. On-site shooting, mass homicide	2
9. Key employee death(s)	2
10. Theft (physical non-cyber)	3
11. Electrical grid outage – area blackout	3
12. Financial systems (Wall Street, central trading areas) outage	3
13. Key employee disabilities	3
14. Key supplier interruption or termination	3
15. Sudden, no access to our primary office location	3
16. Telecommunications outage	4

Event	Severity Level
17. Key client interruption or termination	4
18. Major regulatory changes	4
19. Legal issues such as lawsuits, complaints, regulatory sanctions	5
20. Mass employee exodus	6
21. Custodians and/or key vendors cut off access	6

BIA Report

The Firm has identified the mission critical tasks for the people, processes, and systems to run the Firm's business. The Firm has organized the most crucial tasks and further prioritized them in the order of most critical and timely Mission Critical ("**MC**") code of 3 to mid-level code of 2 to the least critical and timely code of 1.

The Firm established the following durations in terms of the maximum time the Firm could maintain an adequate level of service before some level of damage could start to occur:

MC Code	Maximum Time Offline
3	up to 2 weeks
2	up to 30 days
1	up to 90 days

Mission Critical Relationships and Systems

The Firm has two sides to its business platform: 1) Wealth management for individual accounts and 2) Retirement plans. The diagrams illustrate what the Firm's internal and external resources use to guide through various levels of operation and recovery that could occur.

Wealth Management Platform

Primarily consists of the following:

1. Qualified custodial systems.
2. Marketing systems.
3. Compliance systems.
4. IT support and websites.
5. CRM systems.
6. Billing systems.
7. Reporting systems.
8. Accounting systems.
9. Risk and investment performance related systems.

Retirement Plans Platform

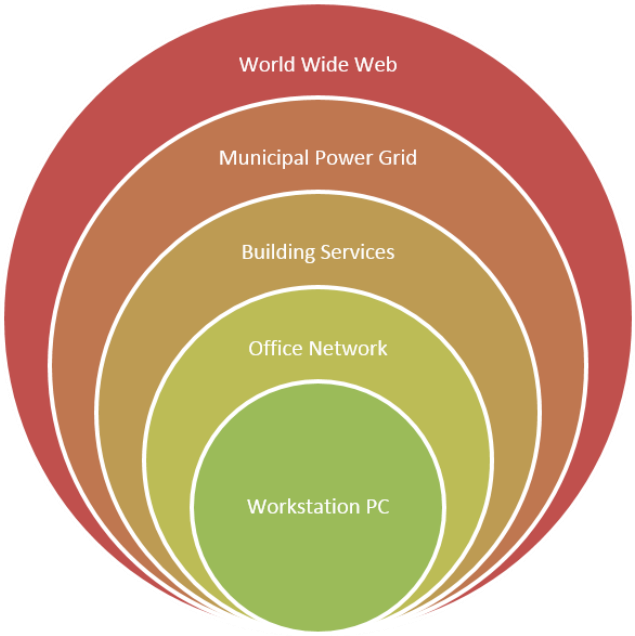
Primarily consists of the following:

1. Recordkeeping systems.
2. Investment monitoring systems.
3. IT support and websites.

4. Billing systems.

From a macro level, basic service (power and communications) standpoint, the Firm has plans in place to deal with various levels of outages. The plans assume layers of services, some of which are outside the realm of possibility and likewise outside the realm of the Firm's ability to do anything about them.

In the diagram (below) the World Wide Web and Municipal Power Grid rings are both less likely to happen and less likely to have long term sustainable backup plans in place to remedy them. The Building Services ring is minimized by the Firm's diesel generator that is on-site at its primary office, which can provide power for as long as the generator can run.



For backup planning purposes, the Firm has procedures in place to deal with outages in the Office Network and Workstation PC rings. These rings are not only impacted by power and utilities, the Firm also has protection in place for:

1. Viruses
2. Spam
3. Ransomware
4. Bots (sitting on server well in advance of breach)
5. Spyware

Tasks with highest Mission Critical (MC) code of 3:

1. Trades.
2. Money movement.
3. Investment Committee.

Tasks with medium Mission Critical score of 2:

1. Client onboarding.
2. Accounts payable.
3. Quarterly performance reporting.
4. The Firm's websites.

Tasks with lowest Mission Critical score of 1:

1. Redtail workflow management.
2. Riskalyze analysis and proposal generation.
3. E-Valuator portfolio management.
4. E-Valuator analysis and proposal generation.
5. Orion systems operations.
6. Advisor onboarding.
7. Advisor training and setup.
8. Board meetings.
9. Company meetings.
10. Web based tools – Mailchimp, WIX, Wystia, Zoom, and CMS system.
11. Compliance – key recurring processes:
    a. Email monitoring.
    b. Social media monitoring.
    c. Wed site monitoring.
    d. Marketing reviews.
    e. Advisor office examinations.

27. PAY TO PLAY POLICY

Statement of Policy

The Firm, as a matter of policy and practice, and consistent with industry best practices, Advisers Act and the SEC requirements (Rule 206 (4) – 5 or "The Rule," under the Advisers Act), has adopted the following procedures which are designed to prevent violations of the Rule. These procedures cover all Supervised Persons.

Definitions

For the purpose of the Firm's compliance with Rule 206 (4) -5, the following definitions shall apply:

1. "**Contribution**" means a gift, subscription, loan, advance, deposit of money, or anything of value made for the purpose of influencing an election for a federal, state, or local office, including any payments for debts incurred in such an election. It also includes transition or inaugural expenses incurred by a successful candidate for state or local office.
2. "**Covered Associates**" means:
    a. Supervised Persons, general partners, managing members, executive officers, or other individual with a similar status or function.
    b. Supervised Persons who solicits a government entity (even if not primarily engaged in solicitation activities).
    c. A political action committee controlled by a Supervised Person or the Firm.
3. "**Covered Investment Pool**" means (i) any investment company registered under the Investment Company Act of 1940 that is an investment option of a plan or program of a government entity; or (ii) any company that would be an investment company under section 3(a) of the Act but for the exclusion provided from that definition by section 3(c) (1), section3 (c)(7) or section 3(c)(11) of that Act.
4. "**De Minimis**" means any aggregate contributions of up to $350, per election, to an elected official or candidate for whom the individual is entitled to vote, and up to $150, per election, to an elected official or candidate for whom the individual is not entitled to vote. De Minimis exceptions are available only for contributions by Supervised Persons and not the business itself. Under both exceptions, primary and general elections are considered separate elections.
5. "**Entitled to vote for an official**" means the Supervised Person's principal residence is in the locality in which the official seeks election.
6. "**Government entity**" means any U.S. state or political subdivision of a U.S. State, including any agency, authority, or instrumentality of the State or political subdivision, a plan, program, or pool of assets sponsored or established by the State or political subdivision or any agency, authority or instrumentality thereof; and officers, agents, or employees of the State or political subdivision or any agency, authority, or instrumentality thereof, acting in their official capacity. As such, government entities include all state and local governments, their agencies and instrumentalities, and all public pension plans and other collective government funds, including participant-directed plans such as 403 (b), 457 and 529 plans.

7. An "**official**" means an incumbent, candidate or successful candidate for elective office of a government entity if the office is directly or indirectly responsible for, or can influence the outcome of, the hiring of a Supervised Person or has the authority to appoint any person who is directly or indirectly responsible for or can influence the outcome of the hiring.
8. "**Political contribution**" means any gift, subscription, loan advance, deposit of money, or anything of value made for the purpose of influencing an election for a federal, state or local office, including any payments for debts incurred in such an election.
9. "**Solicit**" means, with respect to advisory services, to communicate, directly or indirectly, for the purpose of obtaining or retaining a client for, or referring a client to, a Supervised Person.

Regulatory Requirement

In July 2010, the SEC adopted Rule 206(4)-5 which was designed to prevent "pay-to-play" abuses in the industry. The rule applies to any SEC-registered IAR. Rule 206 (4)-5 makes it unlawful for a Supervised Person to:

1. Receive compensation for providing advisory services to a government entity for a 2-year period after they make a political contribution of more than de Minimis amounts to a public official of a government entity or candidate for such office that is in a position to influence the award of advisory business.
2. Pay third parties to solicit government entities for advisory business unless such third parties are registered broker dealers or registered investment advisors (which subject such solicitors to pay-to-play restrictions themselves under SEC rules or FINRA rules).
3. Solicit or coordinate (i) contribution to an official of a government entity to which they are seeking to provide advisory services; or (ii) payments to a political party of a state locality where they are providing or seeking to provide advisory services to a government entity.
4. Do anything indirectly which, if done directly, would result in a violation of the Rule.

Each of the above prohibitions extends to a Supervised Person that manages assets of a government entity through a Covered Investment Pool.

The Rule also contains a look-back provision which attributes to contributions made by a Supervised Person within two years (or 6 months if the person does not solicit business) of becoming a Supervised Person. That is, when a person becomes a Supervised Person, they must "look back" in time to their contributions to determine whether the time out applies. Therefore, if a contribution greater than de Minimis was made less than two years (or six months) from the time the person becomes a Supervised Person, the rule prohibits the contributing Supervised Person from receiving compensation for providing advisory services from the hiring or promotion date until two-year period has run.

Finally, the Rule provides an exception that provides Supervised Persons with limited ability to ensure the consequences of making an inadvertent political contribution to an official for whom they are not entitled to vote (i.e. under the Rule, limited to a $150 contribution per

election). The exception is available for contributions that, in the aggregate, do not exceed $350 to any one official, per election. The Supervised Person must have discovered the contribution which resulted in the prohibition within four months of the date of such and, within 60 days after learning of the triggering contribution, the contributor must obtain the return of the contribution. However, the Supervised Person is limited to relying on this exception to three such events per 12-month period if it has more than 50 employees who perform advisory functions (as reported on Item 5A of Form ADV Part I), and two such events per 12-month period if it has less than 50 employees who perform advisory functions.

Corresponding amendments to Rule 204-2 regarding book and record-keeping requirements also require every SEC-registered Supervised Person to maintain (in addition to other 204-2 requirements) the following:

1. The names, titles, and business and residence addresses of all employees.
2. All government entities to which they provide or have provided advisory services, or which are or were investors in any Covered Investment Pool to which they provide or have provided advisory services, as applicable, in the past five years.
3. All direct or indirect contributions made to an official of a government entity, or payments to a political party of a state or political subdivision thereof, or to a political action committee; and
4. The name and business address of each regulated person to whom they provide or agrees to provide, directly or indirectly, payment to solicit a government entity for advisory services on its behalf.

A Supervised Person's records of contributions and payments are required to (1) be listed in chronological order, (2) identify each contributor and recipient, (3) identify the amounts and dates of each contribution or payment, and (4) identify whether such contribution or payment was subject to the exception for certain returned contribution.

Procedures

Supervised Persons are required to maintain compliance with the Rule and the following procedures apply:

1. Are required to approve any political contributions with Compliance prior to making such a contribution.
2. New Supervised Person's, within 5 business days of employment, are required to provide Compliance with a list indicating to whom they have made any political contributions in the 2 years (either directly or via a political action committee which the employee controls) preceding the date of employment with the Firm.
3. Supervised Persons are responsible for monitoring all political contributions made.
4. Compliance must be aware of any potential solicitation agreements (i.e. prior to signing of the agreement) with third parties to ensure that such meet Rule registration requirement.
5. Compliance is responsible for providing adequate training to Supervised Persons with respect to all Rule requirements.
6. Compliance is responsible for ensuring that all books and records requirements pursuant to Rule 204-2 with respect to political contributions are met and maintained.

28. DOCUMENT DESTRUCTION POLICY

Introduction

The Firm is required to create and retain several documents and records ("**records**") under various legal, regulatory, contractual and general business obligations. The Advisers Act requires all Supervised Persons to adhere to extensive recordkeeping requirements. In addition to creating and maintaining records, it is important for Supervised Persons to destroy records periodically when they are no longer necessary. In some cases, such destruction can be legally or contractually required. The policy below outlines policies concerning document destruction.

Administration & Supervision of Records Retention and Destruction

The CCO oversees the administration of the document destruction policies and the implementation of the processes and procedures to ensure that records are maintained for the appropriate period and the appropriate processes and procedures are followed for the destruction of records.

Suspension of Record Disposal in Event of Litigation or Claims or Regulatory Inquiry

Certain circumstances require the destruction of documents be suspended with respect to a group or class of documents. In the event a Supervised Person is served with any subpoena or request for documents or they become aware of a governmental investigation, audit, or the commencement of any litigation, the Supervised Person is required to inform Compliance immediately and any further disposal of documents shall be suspended until the CCO, with the advice of legal counsel, determines otherwise.

Federal law makes it a crime, punishable by imprisonment and monetary fines, for anyone who knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record or document with the intent of impeding, obstructing, or influencing an investigation or administrative proceeding within the jurisdiction of any department or agency of the United States. The destruction of documents while an investigation or litigation is ongoing or anticipated can also constitute obstruction of justice or lead to monetary sanctions or other penalties. Liability for such conduct depends upon the facts and circumstances but it is best to err on the side of caution and to cease the deletion, destruction, or alteration of any records when an investigation or litigation is anticipated or ongoing.

If a Supervised Person is in doubt as to whether a record pertains to the subject matter of an investigation, litigation, proceeding or foreseeable claim they should not destroy the record unless they receive authorization to do so from Compliance.

Policy Statement

The Firm's policy is to effectuate an orderly, efficient, and documented destruction of specified records. Certain records are maintained for specified periods of time, as required by applicable laws, regulations or contractual obligations. A duty to maintain the record can also exist if it is reasonably foreseeable that such record can be used as evidence in a trial.

During these periods of time, the Supervised Person and the Firm have a legal obligation to preserve the property.

The Supervised Person's and the Firm's documents are managed in accordance with the Document Management Process and documents are destroyed only in accordance with this process.

Purpose of Policy

The Firm is committed to the effective management of records in accordance with legal and contractual requirements, the optimal use of its space and resources, and the elimination and destruction of outdated and unnecessary records. Consistent with those commitments, the purpose of this Document Management Process is to mandate appropriate policies or memorandum of documents to destroy and inform all Supervised Persons the document destruction policies and procedures.

No policy can, however, adequately cover every document management issue or situation. It is possible that documents are not covered by any stated policy. Any questions concerning document creation, retention or destruction that is not answered in this document should be referred to Compliance. The Firm's record retention and destruction policies are always subject to review, update, and change.

Procedure for Destruction of Records

The Firm has created a formal Document Management Process that is used when documents are to be destroyed and the timeline is detailed as follows:

1. **Destruction of "Hard" Copies**
   Destruction of applicable "hard" copies (i.e., documents not maintained in electronic form) can be accomplished using a third-party specializing in shredding and record destruction services. Documents must be shredded rather than placed in a rubbish bin. A record is not considered "destroyed" until it is physically destroyed.
2. **Retirement and Destruction of Computer Hardware**
   Computer hardware and devices being replaced or retired as an asset are reviewed by the appropriate IT resource for any further practical deployment. Computers, including, but not limited to, CPUs and laptops, designated for donation or recycling, and containing Firm information on hard disk drives, are first to have the hard disk drives removed from the computers and be physically destroyed in a manner not permitting the drives to ever be powered on, or data platters within from having stored data accessed. In the event a hard drive is not able to be removed from a device, steps must be taken to permanently erase, reset, or destroy the information contained on the device so that the data cannot be accessed. This policy shall apply to all devices capable of storing information including, but not limited to, External USB Hard Drives, solid state "Flash Drives" or "Thumb Drives," tablets such as iPads, smart telephones, or similar devices. Computers and devices now without internal Hard Disk Drives, or having been appropriately erased or reset, can be recycled or donated at the Supervised Person's discretion.

29. CHARITABLE GIVING POLICY

Introduction

The Firm sets forth policies and procedures to be followed by Supervised Persons with respect to charitable giving. All Supervised Persons of the Firm are subject to this policy.

Policy

Supervised Persons can make charitable contributions on their own behalf as an individual but are prohibited from associating their business or the Firm's name with such contributions or payments. Supervised Persons are required to follow these general principles when making donations to charities sponsored by clients.

Charitable contributions must be pre-approved by Compliance if:

1. Solicited or directed by clients or prospective clients.
2. Made on behalf of clients or prospective clients.
3. Made for the purpose of influencing the award or continuation of a business relationship with a client or prospective client.

All charitable contributions that are not clients can be contributed and do not require pre-approval from Compliance, unless the total contribution is more than $5,000 USD. All charitable contributions greater than $5,000 USD must be pre-approved by Compliance.

Any questions as to the appropriateness of charitable contributions should be discussed with Compliance.

30. OVERSIGHT OF SERVICE PROVIDERS

Introduction

The Firm contracts with outside vendors to perform certain functions for the Firm. The Firm never contracts its supervisory and compliance activities away from its direct control, it does outsource certain activities that support the performance of its supervisory and compliance responsibilities. Such activities include Qualified Custodians, sub-advisors, email monitoring and retention, social media and monitoring, accounting and finance, legal, compliance support, information technology, disaster recovery services, marketing, and cybersecurity.

The CCO oversees the Firm's service providers that impact the operations or that could pose a risk to the Firm's operations or its clients ("**service provider**"). The CCO is familiar with each service provider's operations and understand the aspects of their operations that expose the Firm to compliance risks. The Firm follows the policies and procedures established by the service provider after the Firm confirms they are in line with their operations.

Service Provider Evaluation

The Firm evaluates the service provider's ability to fulfill the services needed. Each service provider agreement outlines the scope of the provider's responsibilities. The service provider's written agreement is maintained by the CCO in accordance with the Firm's Document Management Process. Agreements properly reflect protection of any confidential information, including, but not limited to, that of the Firm, as well as nonpublic client information. Agreements must be maintained, must be current, and must be available for review by regulators, when requested. If the agreement does not contain a confidentiality agreement, the Firm obtains a separate agreement to be maintained in the file with the vendor contract and in accordance with the Firm's document retention policy.

When conducting due diligence on a service provider for the first time, the CCO reviews and considers the following information, as applicable:

1. The service provider's history and reputation in the industry, including the experiences of similar entities serviced by this provider and the provider's history of client retention.
2. The service provider's financial condition and ability to devote resources to the Firm.
3. Recent corporate transactions (such as mergers and acquisitions) that involve the service provider.
4. The level of service that is provided.
5. The nature and quality of the services to be provided.
6. The extent to which, if at all, the service provider adopts and abides by Global Investment Performance Standards ("**GIPS**").
7. The experience and quality of the staff providing services and the stability of the workforce.
8. The service provider's operational resiliency, including its disaster recovery and business continuity plans.

9. The technology and process it uses to maintain information security, including the privacy of client data and its cybersecurity policies and procedures.
10. The service provider's communications technology.
11. The service provider's literature and advertising.
12. The service provider's insurance coverage.
13. The reasonableness of fees in relation to the nature and extent of the services to be provided.

Service Provider Monitoring

The CCO shall be responsible for monitoring all service providers on an annual basis to ensure compliance with the terms and conditions of the agreement. The CCO documents the monitoring assessment and includes the following:

1. The service provider's financial condition and ability to devote resources.
2. Recent corporate transactions (such as mergers and acquisitions) that involve the service provider.
3. The level of service provided.
4. The service provider's performance to date.
5. The extent to which the service provider abides by GIPS.
6. The reasonableness of fees in relation to the nature and extent of the services to be provided.
7. The potential for conflicts of interest to the detriment of clients.
8. The experience and quality of the staff providing services and the stability of the workforce.
9. The service provider's operational resiliency, including its disaster recovery and business continuity plans.
10. The technology and process it uses to maintain information security, including the privacy of client data as well as its cybersecurity processes.
11. The service provider's communications.

Where potential conflicts of interest exist, the CCO must evaluate the extent to which such potential conflicts are mitigated.

When evaluating an arrangement with an affiliated service provider that in turn subcontracts to an unaffiliated service provider, the CCO shall inquire about the respective roles of the two entities and whether management or the affiliated service provider receives any benefit, directly or indirectly, other than the fees payable under the contract. The CCO evaluates the fees paid to the affiliated service provider and any unaffiliated service provider, relative to the services each performs.

APPENDIX A – RETENTION OF BOOKS AND RECORDS

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
1. Form ADV, Part 2A and Appendix 1	Advisers Act	Rule 204-1(c)	Permanently (per law: none specified)	None Specified	Paper, microfilm, electronic	Part 2A of Form ADV
1. Articles of Incorporation	Advisers Act	Rule 204-2(e)(2)	Permanently; 3 years after termination of business	Onsite (principal office of Supervised Person)	Paper, microfilm, electronic	Partnership articles and any amendments thereto, articles of incorporation, charters, minute books, and stock certificate books.
2. Bylaws	Advisers Act	Rule 204-2(e)(2)	Permanently; 3 years after termination of business	Onsite (principal office of Supervised Person)	Paper, microfilm, electronic	Partnership articles and any amendments thereto, articles of incorporation, charters, minute books, and stock certificate books.
3. Minute Books	Advisers Act	Rule 204-2(e)(2)	Permanently; 3 years after termination of business	Onsite (principal office of Supervised Person)	Paper, microfilm, electronic	Partnership articles and any amendments thereto, articles of incorporation, charters, minute books, and stock certificate books.
4. Stock Certificate Book	Advisers Act	Rule 204-2(e)(2)	Permanently; 3 years after termination of business	Onsite (principal office of Supervised Person)	Paper, microfilm, electronic	Partnership articles and any amendments thereto, articles of incorporation, charters, minute books, and stock certificate books.
5. Accounting Journals	Advisers Act	Rule 204-2(a)(1), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	A journal or journals, including cash receipts and disbursement records, and any other records of original entry forming the basis for entries in any ledger.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
6. Accounting Ledgers	Advisers Act	Rule 204-2(a)(2), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	General and auxiliary ledgers (or other comparable records) reflecting asset, liability, reserve, capital, income, and expense accounts.
7. Accounting Bank Statements	Advisers Act	Rule 204-2(a)(4), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All check books, bank statements, canceled checks, and cash reconciliation of the Supervised Person.
8. Accounting Bills or Statements	Advisers Act	Rule 204-2(a)(5), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All bills or statements (or copies thereof), paid or unpaid, relating to the business of the Supervised Person.
9. Accounting Financial Statements	Advisers Act	Rule 204-2(a)(6), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All trial balances, financial statements, and internal audit working papers relating to the business of the Supervised Person.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
10. Trade Tickets Memorandum	Advisers Act	Rule 204-2(a)(3), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	A memorandum of each order given by the Supervised Person, any instruction received by the Supervised Person from the client, and any modification or cancellation of any such order or instruction relating to the purchase or sale of any security.
11. Recommendations	Advisers Act	Rule 204-2(a)(7), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	Originals of all written communications received and sent by the Supervised Person relating to any recommendation made or proposed to be made and any advice given or proposed to be given.
12. Delivery Instructions	Advisers Act	Rule 204-2(a)(7), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	Originals of all written communication received, and copies of all written communications sent by the Supervised Person and relating to any receipt, disbursement or delivery of funds or securities.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
13. Trade Confirmation	Advisers Act	Rule 204-2(a)(7), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	Originals of all written communication received, and copies of all written communications sent by the Supervised Person relating to the placing or execution of any order to purchase or sell any securities.
14. List of Discretionary Accounts	Advisers Act	Rule 204-2(a)(8), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	A list or other record of all accounts in which the Supervised Person is vested with any discretionary power with respect to the funds, securities or transactions of any client.
15. Powers of Attorney	Advisers Act	Rule 204-2(a)(9), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All powers of attorney and other evidence of the granting of any discretionary authority by any client to the Supervised Person, or copies thereof.
16. Advisory Agreements (Funds)	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
17. Sub-advisory Agreements (Funds)	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
18. Advisory Agreements (Managed Accounts)	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
19. Advisory Agreements (Commingled Fund Accounts)	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
20. Subscription Agreements (Commingled Funds)	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
21. Alliance Agreements	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
22. Pricing Vendor Agreements	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
23. Soft Dollar Agreements	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
24. Directed Brokerage Agreements	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
25. Employment Agreements	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
26. Leases	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
27. Other Agreements	Advisers Act	Rule 204-2(a)(10), Rule 204-2(e)(1) Also applies if fund is a party: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written agreements (or copies thereof) entered by the Supervised Person with any client or otherwise relating to the business of the Supervised Person as such.
28. Sales Literature General	Advisers Act	Rule 204-2(a)(11), Rule 204-2(e)(3) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from last use (per law: end of fiscal year of)	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	A copy of each notice, circular, advertisement, newspaper article, investment letter, bulletin, or other communication circulated to 10 or more persons.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
29. Sales Literature Backup	Advisers Act	Rule 204-2(a)(16), Rule 204-2(e)(3) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	If needed to support performance (per law: not less than 5 years from end of fiscal year of last use)	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All accounts, books, internal working papers, and any other records or documents that are necessary to form the basis for or demonstrate the calculation of the performance or rate of return of any or all managed accounts or securities recommendations used in any sales literature.
30. Personal Transaction Reports Confirmations	Advisers Act	Rule 204-2(a)(12), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	A record of every transaction in a security in which the Supervised Person or any representative of the Supervised Person has, or by reason of the transaction acquires, any direct or indirect beneficial ownership.
31. Written Disclosure Statement (Part II of Form ADV)	Advisers Act	Rule 204-2(a)(14), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	A copy of each written statement and amendment or revision given or sent to any client or prospective client in accordance with provisions of Rule 204-3 and a record of the dates that each written statement was given or offered to be given to any client or prospective client.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
32. Solicitor Documents	Advisers Act	Rule 204-2(a)(15), Rule 204-2(e)(1)	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	All written acknowledgements of receipt obtained from clients pursuant to the solicitor's rule and copies of disclosure documents delivered to clients by solicitors pursuant to Rule 206(4)-3.
33. Client Account Records	Advisers Act	Rule 204-2(c)(1), Rule 204-2(e)(1) Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	5 years from end of fiscal year in which last entry was made	Onsite (2 years), offsite remainder (per law: 5 years easily accessible and 2 years in appropriate office of Supervised Person)	Paper, microfilm, electronic	Records showing separately for each such client the securities purchased and sold, and the date, amount and price of each such purchase and sale.
34. Position Reports	Advisers Act	Rule 204-2(c)(2), Also applies: 1940 Act Rules 31a-1(f), Rule 31a-1(e) – 6 years	None Specified	None specified	Paper, microfilm, electronic	For each security in which any such client has a current position, information from which the Supervised Person can promptly furnish the name of each such client, and the current amount or interest of such client.
35. Form ADV and all amendments	Advisers Act	Section 204	Permanently (per law: none specified)	None specified	None specified	Not addressed but recommended.
36. Form ADV-S	Advisers Act	Section 204	Permanently (per law: none specified)	None specified	None specified	Not addressed but recommended.
37. Other Filings (e.g., Form ADV-Y2K)	Advisers Act	Section 204	Permanently (per law: none specified)	None specified	None specified	Not addressed but recommended.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
38. Insider Trading Policy	Advisers Act	Section 204A	Permanently (per law: none specified)	None specified	None specified	Not addressed but recommended.
39. Allocation Procedures	Advisers Act	General Fiduciary Standards	Permanently	None specified	None specified	Not addressed but recommended.
40. Trading Error Procedures	Advisers Act	General Fiduciary Standards	Permanently	None specified	None specified	Not addressed but recommended.
41. Pricing Procedures	Advisers Act	General Fiduciary Standards	Permanently	None specified	None specified	Not addressed but recommended.
42. Trading Error Correction Procedures	Advisers Act	General Fiduciary Standards	Permanently	None specified	None specified	Not addressed but recommended.
43. Proxy Voting Procedures	Advisers Act, ERISA	General Fiduciary Standards	Permanently	None specified	None specified	Not addressed but recommended.
44. Ethics Code Records	1940 Act	Rule 17j-1(f)(1)(A)-(E)	All records required under Rule 17j-1. See books and records chart for registered investment companies.			
45. Rule 204-2 Records	1940 Act	Rule 31a-1(f) Rule 31a-2(e)	6 years	None specified	Paper, microfilm, electronic	Such accounts, books, records, and other documents required to be maintained pursuant to Rule 204-2 to the extent necessary or appropriate to record such person's transaction with each registered investment company.
46. Schedule 13Gs & 13Ds	1934 Act	Rule 13d-1	Permanently (per law: none specified)	None specified	None specified	Not addressed but recommended.

Record Type	Name of Law	Legal Cite	Retention Period	Record Retention	Storage Media	Summary of Law
47. Soft Dollar Allocations	1934 Act	Section 28(e)	Permanently	None specified	None specified	Internal records supporting allocation of mixed-use items (recommended).
48. Privacy Notices	Regulation S-P	Section 248.9	Permanently	None specified	None specified	Not addressed but recommended.
49. Privacy Procedures	Regulation S-P	Section 248.30	Permanently	None specified	None specified	Not addressed but recommended.
50. Advisory Representative Licensing	Blue Sky Law	Varies by State	Permanently	None specified	None specified	Not addressed but recommended.
51. Notice fillings	Blue Sky Law	Varies by State	Permanently	None specified	None specified	Not addressed but recommended.
52. Renewal fillings	Blue Sky Law	Varies by State	Permanently	None specified	None specified	Not addressed but recommended.

APPENDIX B – INSIDER TRADING

STATEMENT OF POLICIES AND PROCEDURES WITH RESPECT TO THE FLOW AND USE OF MATERIAL NONPUBLIC (INSIDE) INFORMATION

This is a Statement of Policies and Procedures with Respect to the Flow and Use of Material Nonpublic (Inside) Information (the "**Statement**") of the Firm.

A reputation for integrity and high ethical standards in the conduct of the affairs of the Firm is of paramount importance. To preserve this reputation, it is essential that all transactions in securities be affected in conformity with applicable securities laws.

This Statement has been adopted in response to the requirements of the Insider Trading and Securities Fraud Enforcement Act of 1988 (the "**Act**"). The Act was designed to enhance the enforcement of the securities laws, particularly in the area of insider trading, by (i) imposing severe penalties on persons who violate the laws by trading on material, nonpublic information and (ii) requiring Supervised Persons to establish, maintain, and enforce written policies and procedures reasonably designed to prevent the misuse of inside information. All Supervised Persons of the Firm are required to comply with this Statement.

The purpose of this Statement is to explain: (1) the general legal prohibitions regarding insider trading; (2) the meaning of the key concepts underlying the prohibition; (3) the sanctions for insider trading and expanded liability for controlling persons; and (4) the Firm's educational program regarding insider trading.

The Basic Insider Trading Prohibition

The Act does not define insider trading. However, in general, the "**insider trading**" doctrine under U.S. federal securities laws prohibits any Supervised Person from knowingly or recklessly breaching a duty owed by:

1. Trading while in possession of material, nonpublic information.
2. Communicating ("**tipping**") such information to others.
3. Recommending the purchase or sale of securities based on such information.
4. Providing substantial assistance to someone who is engaged in any of the aforementioned activities.

In addition, rules of the U.S. Securities and Exchange Commission ("**SEC**") prohibit a Supervised Person from trading while in possession of material, nonpublic information relating to a tender offer, whether or not trading involves a breach of duty, except for a company acting in compliance with "Chinese Wall" (which is a virtual information barrier erected between those who have material, non-public information and those who don't, to prevent conflicts of interest), procedures.

Possession Versus Use of Inside Information (Meaning of "on the basis of")

Until recently, an unsettled issue under U.S. insider trading laws was whether an alleged violator must have "used" material nonpublic information or whether mere "possession" is enough. To clarify this issue, the SEC adopted Rule 10b5-1 under the Securities Exchange Act of 1934, which states that "a purchase or sale of a security of an issuer is "on the basis of" material nonpublic information about that security or issuer if the Supervised Person making the purchase or sale was aware of the material nonpublic information when they made the purchase or sale." In other words, if a Supervised Person trades with respect to a security or issuer while they have knowing possession of material and nonpublic information about the security or issuer, they have traded "on the basis of" that information (in possible violation of insider trading laws) even if they did not actually use the information in making the trade.

Basic Concepts

As noted, the Act did not specifically define insider trading. However, federal law prohibits knowingly or recklessly purchasing or selling directly or indirectly a security while in possession of material, nonpublic information or communicating ("tipping") such information in connection with a purchase or sale. Under current case law, the SEC must establish that the Supervised Person misusing the information has breached either a fiduciary duty to company shareholders or some other duty not to misappropriate insider information.

Thus, the key aspects of insider trading are: (A) materiality, (B) nonpublic information, (C) knowing or reckless action and (D) breach of fiduciary duty or misappropriation. Each aspect is briefly discussed below.

1. **Materiality.** Insider trading restrictions arise only when information that is used for trading, recommending, or tipping is "material." Information is considered "material" if there is a substantial likelihood that a reasonable investor would consider it important in making their investment decisions, or if it could reasonably be expected to affect the price of a company's securities. It need not be so important that it would have changed the investor's decision to buy or sell. On the other hand, not every piece of information about a security is material.
2. **Nonpublic Information.** Information is considered public if it has been disseminated in a manner making it available to investors generally (e.g., national business and financial news wire services, such as Dow Jones and Reuters; national news services, such as The Associated Press, The New York Times or The Wall Street Journal; broad tapes; SEC reports; analysts' reports that have been disseminated to the Firm's clients). Just as an investor is permitted to trade based on nonpublic information that is not material, they can also trade based on information that is public. However, as an example, information given by a company director to an acquaintance of an impending takeover prior to that information being made public would be considered both "material" and "nonpublic." Trading by either the director or the acquaintance prior to the information being made public would violate the federal securities laws.

3. **Knowing.** Under the federal securities laws, a violation of the insider trading limitations requires that the individual act (i) with scienter (which is with knowledge that their conduct can violate these limitations), or (ii) in a reckless manner. Recklessness involves acting in a manner that ignores circumstances that a reasonable person would conclude would result in a violation of insider trading limitations.
4. **Fiduciary Duty.** The general tenor of recent court decisions is that insider trading does not violate the federal securities laws if the trading, recommending, or tipping of the insider information does not result in a breach of duty. Over the last decade, the SEC has brought cases against accountants, lawyers, and stockbrokers because of their participation in a breach of an insider's fiduciary duty to the corporation and its shareholders. The SEC has also brought cases against non-corporate employees who misappropriated information about a corporation and thereby allegedly violated their duties to their employers. The situations in which a person can trade on the basis of material, nonpublic information without raising a question whether a duty has been breached are so rare, complex and uncertain that the only prudent course is not to trade, tip, or recommend while in possession of or based on inside information. In addition, trading by an individual while in possession of material, nonpublic information relating to a tender offer is illegal irrespective of whether such conduct breaches a fiduciary duty of such individual. Set forth below are several situations where courts have held that such trading involves a breach of fiduciary duty or is otherwise illegal.

Corporate Insider. In the context of interviews or other contact with corporate management, the Supreme Court held that an investment analyst who obtained material, nonpublic information about a corporation from a corporate insider does not violate insider trading restrictions in the use of such information unless the insider disclosed the information for "personal gain." However, personal gain can be defined broadly to include not only a pecuniary benefit, but also a reputational benefit or a gift. Moreover, selective disclosure of material, nonpublic information to an analyst might be viewed as a gift.

Tipping Information. The Act includes a technical amendment clarifying that tippers can be sued as primary violators of insider trading prohibitions, and not merely as aiders and abettors of a tipper's violation. In enacting this amendment, Congress intended to make clear that tippers cannot avoid liability by misleading their tippers about whether the information conveyed was nonpublic or whether their disclosure breached a duty. However, Congress recognized the crucial role of securities analysts in the smooth functioning of the markets and emphasized that the new direct liability of tippers was not intended to inhibit "honest communications between corporate officials and securities analysts."

Corporate Outsider. Additionally, liability could be established when trading occurs based on material, nonpublic information that was stolen or misappropriated from any other person, whether a corporate insider or not. An example of an area where trading on information can give rise to liability, even though from outside the company whose securities are traded, is material, nonpublic information secured from an attorney or investment banker employed by the company.

Tender Offers. The SEC has adopted a rule specifically prohibiting trading while in possession of material information about a prospective tender offer before it is publicly announced. This rule also prohibits trading while in possession of material information during a tender offer which a person knows or has reason to know is not yet public. Under the rule, there is no need for the SEC to prove a breach of duty. Furthermore, in the SEC's view, there is no need to prove that the nonpublic, material information was actively used in connection with trading before or during a tender offer. However, this rule has an exception that allows trading by one part of a securities firm where another part of that firm has material, nonpublic information about a tender offer if certain strict Chinese Wall procedures are followed.

Sanctions and Liabilities

Sanctions

Insider trading violations can result in severe sanctions being imposed on Supervised Persons and on the Firm. These could involve SEC administrative sanctions, such as being barred from employment in the securities industry, SEC suits for disgorgement and civil penalties of, in the aggregate, up to three times profits gained or losses avoided by the trading, private damage suits brought by persons who traded in the market at about the same time as the person who traded on inside information, and criminal prosecution which could result in substantial fines and jail sentences. Even in the absence of legal action, violation of insider trading prohibitions or failure to comply with this Statement or the Code of Ethics can result in termination of employment and referral to the appropriate authorities.

Controlling Persons

The Act increases the liability of "controlling persons" defined to include both an employer and any person with the power to influence or control the activities of another. For example, any individual that is a manager or director or officer exercising policy making responsibility is presumed to be a controlling person. Thus, a controlling person can be liable for another's actions as well as his or her own.

A controlling person of an insider trader or tipper can be liable if such person failed to take appropriate steps once such person knew of or recklessly disregarded the fact that the controlled person was likely to engage in a violation of the insider trading limitations. The Act does not define the terms, but "reckless" is discussed in the legislative history as a "heedless indifference as to whether circumstances suggesting employee violations actually exist."

A controlling person of an insider trader or tipper can also be liable if such person failed to adopt and implement measures reasonably designed to prevent insider trading. This Statement and the Code of Ethics are designed for this purpose, among others.

Restrictions and Required Conduct to Prevent Insider Trading

In order to prevent even inadvertent violations of the ban on insider trading, or even the appearance of impropriety regarding other forms of personal trading, the following standards of conduct are required to be observed:

1. All information about the clients and about securities in which the clients invest, including but not limited to the value of accounts; securities bought, sold, or held; current or proposed business plans; acquisition targets; confidential financial reports or projections; borrowings, etc., must be held in strictest confidence.
2. When obtaining material information about an issuer or portfolio from insiders, the Firm determines whether the information learned has already been disseminated through public channels. In discussions with securities analysts, it is appropriate to determine whether the information the analyst provides has been publicly disseminated.
3. If a Supervised Person suspects that they have learned material, non-public information about an issuer, they must take the following steps:
   a. Report the information and any proposed trade in that security to Compliance.
   b. Do not buy or sell the securities for your own account or for the account of anyone else, including a client.
   c. After reviewing the issue, Compliance decides as to whether the information is "inside" information. If it is, Compliance informs all Supervised Persons, and no one at the Firm can trade based on such information until Compliance determines that the information has been made public. At that time, Compliance notifies all Supervised Persons in writing that the ban on trading based on such information has been lifted.
4. At all times, decisions regarding investments for clients are made independently of decision concerning the accounts of Supervised Persons. Under no circumstances can action be taken for client accounts in order to benefit a Supervised Person's account or those of the Supervised Person's Family/Household.
5. Supervised Persons are prohibited from recommending any securities transaction for a client without having disclosed their interest, if any, in such securities or the issuer of the securities, including without limitation: (1) their direct or indirect beneficial ownership of any securities of such issuer; (2) whether they contemplate a transaction in such securities; (3) if they have any position with such issuer or its affiliates; and (4) if they have any present or proposed business relationship between such issuer or its affiliates or any party in which has a significant interest.

APPENDIX C – DOCUMENT MANAGEMENT PROCESS FOR THE BUSINESS

Purpose

The purpose of this policy is to assist Supervised Persons in managing all documents produced in the operation of the Firm. This Policy excludes any client documents already covered in this Compliance Manual. The Firm provides a clear and comprehensive understanding of which documents contain confidential information and how to manage, store, and securely destroy them. In addition, the Firm provides clear guidance as to which documents are legislated to be retained for requisite periods of time and the procedures governing their maintenance. The Firm requires Supervised Persons to:

1. Retain important documents for reference and future use.
2. Dispose of documents that are no longer necessary through secure destruction and recycling containers.
3. Organize important documents for efficient retrieval.
4. Know what documents should be retained, the length of their retention, means of storage, and when and how they should be destroyed.
5. Comply with laws regarding the retention of records and data.
6. Ensure information is available for legal investigations or actions as required.

Implementation of, and compliance with the policy is essential to its effectiveness. Incomplete or selective implementation exposes Supervised Persons to legal risks and termination. Should any questions, comments, or suggestions arise regarding this policy, contact Compliance.

Scope

This policy applies to all printed and electronic documents, confidential information, and general Firm information (as defined below and excluding client documents already covered in this Compliance Manual) belonging to the Supervised Person or to which the Supervised Person is a party or signatory.

Responsibilities

Compliance is responsible for ensuring that this policy is followed. All Supervised Persons are responsible for complying with this policy.

Definitions

1. **Documents and Records (used interchangeably)**. Refers to all Firm records including written, printed, as well as electronic records (i.e., e-mails and documents saved electronically). Documents and records include, but are not limited to, papers, copies, drafts, bound records, drawings, maps, photographs, electronic communications, and any other physical devices containing information, including electronic storage devices.
2. **Confidential Information.** All information that is produced in the course of business that is not available from public sources is considered confidential. This includes any or all documents or files that contains business, partner or employee names, pricing, and personal information. This also includes private information on individuals as defined

by privacy and identity theft legislation, as well as information that is available as a result of the Firm's practice(s), but which is not generally known or readily obtainable by others outside of the Firm but can be used in general throughout the Firm.

3. **General Firm Information.** General Firm information documents include, but are not limited to:

• Accounting documents • Information technology documents • General Contracts • Internal reports • Payroll statements • Training information and manuals • Executive level budgets • Legal contracts • Strategic reports • Health and safety records • Medical records • Payroll information • Performance appraisals • Human Resources documents	• Corporate legal records • Supplier purchase orders • Supplier records • Supplier specifications • Research and development reports • Performance appraisals • Product testing and results • Product development plans • Sales and marketing reports • Specifications and drawings • Internal communications • Advertising materials • Business strategies

4. **Electronic Storage Device.** Refers to any and all electronic storage devices that are provided by or contain information that is the property of the Firm, are under the control of the Firm, and are used by any of the employees of the Firm, contractors, officers, or directors. Electronic Storage Devices include personal computers, servers, laptops, related storage devices such as hard drives, flash drives, and CDs.

Storage of Records and Documents

1. **Tangible Records.** Tangible records that do not contain confidential information are those that can be physically moved to storage such as paper records (including printed versions of electronically saved documents), photographs, investor presentations, and promotional items, etc. These active, tangible records and documents that need to be easily accessible are stored in a secure storage facility.
2. **Confidential Information.** Records and documents that contain confidential information but are in use should be stored in a locked storage drawer/cabinet. Each employee of the Firm should be provided with at least one lockable drawer/cabinet to store documents that are prohibited from being out in the open (such as any document that contains client personal information or account numbers). All confidential information shall be kept out of view from unauthorized personnel and locked up when not in use.
3. **Inactive documents.** These records can be sent to a secure off-site storage facility. This off-site storage facility must be evaluated for security and reliability.

4. **Legal and Financial Regulations.** Please note that in some jurisdictions and domains, human resource, legal, and financial documents can have specific rules and regulations governing their retention, distribution, storage, and destruction. Contact Compliance for specific information, direction, and practices regarding those documents.